

# **ShAir Office**

## **Multi-Function**

### **Internet & Wireless Gateway**

**Models MIL-W0311 & MIL-W1311**

**Broadband Internet Access**

**Wireless Access Point**

**Dial-in RAS**

**Print Server**



---

## **User's Guide**

---

# TABLE OF CONTENTS

---

<b>CHAPTER 1 INTRODUCTION</b> .....	<b>1</b>
Wireless Gateway Features .....	1
Package Contents .....	4
Physical Details .....	4
<b>CHAPTER 2 INSTALLATION</b> .....	<b>8</b>
Requirements .....	8
Procedure .....	8
<b>CHAPTER 3 CONFIGURATION</b> .....	<b>10</b>
Overview .....	10
Configuration Program.....	11
Quick Setup Screen .....	13
Wireless Screen.....	17
Status Screen.....	20
<b>CHAPTER 4 PC CONFIGURATION</b> .....	<b>26</b>
Overview .....	26
Windows Clients .....	26
Macintosh Clients.....	37
Linux Clients.....	38
Other Unix Systems.....	39
Wireless Station Configuration .....	39
<b>CHAPTER 5 DHCP</b> .....	<b>40</b>
Overview .....	40
What DHCP Does.....	40
Using the Wireless Gateway's DHCP Server .....	40
Using another DHCP Server .....	40
To Configure your PCs to use DHCP .....	41
<b>CHAPTER 6 SERIAL PORT</b> .....	<b>42</b>
Overview .....	42
Serial Port Screen.....	42
Modem Properties Screen.....	45
Dial -in Users.....	47
Serial Port Status.....	51
<b>CHAPTER 7 OPTIONS</b> .....	<b>54</b>
Overview .....	54
Password .....	54
DNS (Domain Name Server) .....	55
NAT (Network Address Translation) .....	55
TFTP.....	55
Remote Management.....	55
Routing Table .....	56
Printer Port.....	56
<b>CHAPTER 8 ROUTING</b> .....	<b>58</b>
Overview .....	58
Routing Screen.....	58
Router Configuration.....	60
Static Routing - Example .....	61
<b>CHAPTER 9 ADVANCED INTERNET</b> .....	<b>62</b>
Overview .....	62
Advanced Internet Screen.....	62
Special Internet Applications .....	63

URL Filter .....	66
Virtual Servers.....	68
DMZ.....	73
<b>CHAPTER 10 ACCESS CONTROL.....</b>	<b>75</b>
Overview .....	75
Security Groups Screen.....	76
PCs Screen.....	78
Filters Screen .....	80
<b>APPENDIX A TROUBLESHOOTING .....</b>	<b>81</b>
Overview .....	81
General Problems .....	81
Internet Access.....	81
Wireless Access .....	82
Printing.....	83
Dial-in Access.....	86
<b>APPENDIX B ABOUT WIRELESS LANS .....</b>	<b>88</b>
Modes .....	88
BSS/ESS.....	88
Channels .....	89
WEP .....	89
Access Control .....	90
Wireless LAN Configuration.....	90
<b>APPENDIX C AT COMMANDS.....</b>	<b>91</b>
AT Commands .....	91
Standard AT Commands .....	93
<b>APPENDIX D SPECIFICATIONS.....</b>	<b>96</b>
Wireless Gateway .....	96
PCMCIA Wireless Card (MIL-W1311 only) .....	97

P/N: 9560DP0101

Copyright © 2001. All Rights Reserved.

Document Version: 1.0

All trademarks and trade names are the properties of their respective owners.

# Chapter 1

## Introduction

# 1

*This Chapter provides an overview of the Wireless Gateway's features and capabilities.*

Congratulations on the purchase of your new Wireless Gateway Multi-Function Wireless Gateway. The Wireless Gateway is a multi-function device providing the following services (the wireless functions are only available on the MIL-W1311 or an MIL-W0133 with an MIL-W1897 wireless adapter):

- **Shared Internet Access** via an DSL or Cable modem on the WAN (Ethernet) port, OR via an analog modem or ISDN TA on the Serial (RS232) port.
- **Wireless LAN Access Point** (base station) for equipment compliant with the IEEE802.11b (DSSS) specifications. Available on the MIL-W1311 (MIL-W0311 with MIL-W1897)
- **Network Printer** - LAN and WLAN users can share the printer attached to the Wireless Gateway.
- **RAS Dial-in Access** - Remote users can use the Wireless Gateway to connect to the LAN and access LAN resources, including the Wireless Gateway's printer and Broadband Internet access.

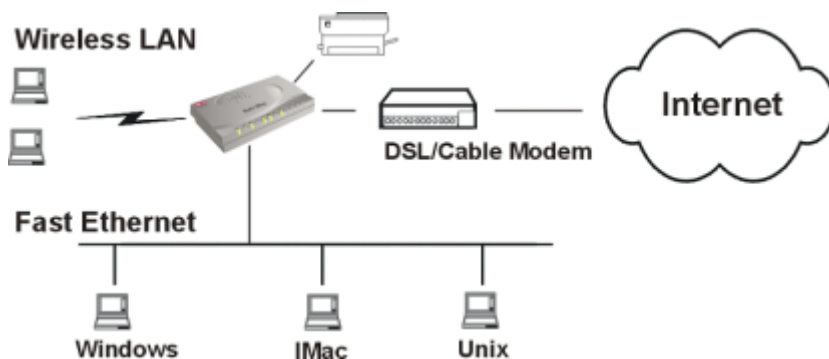


Figure 1: Wireless Gateway

## Wireless Gateway Features

The Wireless Gateway incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

### LAN Features

- **Dual LAN ports.** The Wireless Gateway has two (2) 10/100BaseT Ethernet LAN ports. Normally, the “Hub” port is used to connect the Wireless Gateway to a 10/100BaseT hub on your LAN. But if desired, the “PC” port can be used to connect the Wireless Gateway directly to your PC, using a standard LAN cable.
- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The Wireless Gateway can act as a **DHCP Server** for devices on your local LAN and WLAN.

- **Multi Segment LAN Support.** LANs containing one or more segments are supported, via the Wireless Gateway's built-in static routing table. If NAT (Network Address Translation) is disabled, the Wireless Gateway will function as a static router.

## Internet Access Features

- **Shared Internet Access.** All users on the LAN or WLAN can access the Internet through the Wireless Gateway, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- **DSL & Cable Modem Support.** The Wireless Gateway has a 10BaseT Ethernet port for connecting an DSL or Cable Modem. All popular DSL and Cable Modems are supported.
- **Analog Modem and ISDN TA Support.** If you don't yet have Broadband Internet access, the Wireless Gateway can provide shared Internet access via an analog modem or ISDN TA connected to the serial (RS232) port.
- **PPPoE Support.** The WAN port connection can use PPPoE (PPP over Ethernet), if your ISP uses this method.
- **Fixed or Dynamic IP Address.** On the WAN connection, the Wireless Gateway supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

## Wireless Features

- **Standards Compliant.** The Wireless Gateway complies with the IEEE802.11b (DSSS) specifications for Wireless LANs.
- **Security Features.** Support for WEP (Wired Equivalent Privacy) and Access Control is included.
- **Simple Configuration.** If the default settings are unsuitable, they can be changed quickly and easily.

## Network Printer

- **Share your Printer.** A printer connected to the Wireless Gateway's parallel port can be used by all PCs on the LAN.
- **Multiple Operating Systems.** Clients may use any of the following operating systems:
  - Windows 95/98/ME
  - Windows NT 4.0 or 2000
  - Apple Macintosh
  - Unix
- **Multi-protocol Support.** The following printing methods are supported:
  - Windows peer-to-peer printing over TCP/IP, using the supplied port driver.
  - Windows LPD printing, using a Windows Server running NT 4.0 or Windows 2000 Server. In this situation, no software needs to be installed on the client PCs.
  - Unix LPD printing. No additional software needs to be installed.

---

## Advanced Internet Functions

- **Virtual Servers.** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **User-Defined Virtual Servers.** Internet users can access non-standard Internet Servers on your LAN by using this feature.
- **Special Internet Applications.** Internet applications such as Internet Videoconferencing, Telephony, Games Servers, and other special-purpose Servers are supported.
- **DMZ.** One (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet.
- **URL Filter.** Use the URL Filter to block access to undesirable Web sites by LAN users, Wireless LAN users, or the Dial-in user.
- **Internet Access Log.** See which Internet connections have been made.

## RAS (Remote Access Services)

- **RAS Dial-in.** Remote PC users can use their standard Dial-up software to connect to the Wireless Gateway and access LAN resources.
- **Dial-back Support.** For additional security, the Dial-back feature can be used to hang up and re-dial the remote user. Both fixed and roaming options are supported.

## Configuration & Management

- **Easy Setup.** Use your WEB browser from anywhere on the LAN for configuration.
- **Remote Management.** The Wireless Gateway can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.

## Security Features

- **Configuration Data.** Optional password protection is provided to prevent unauthorized users from modifying the configuration.
- **Access Control Features.** The LAN Administrator can limit Internet access by individual workstations. And the *Access Control* log allows the Administrator to see attempted accesses which have been blocked.
- **Wireless LAN Security.** WEP (Wired Equivalent Privacy) is supported, as well as Wireless access control via station address.
- **Firewall Protection.** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources. (This protection is lost if NAT is disabled.)

### **NAT Firewall Protection**

The firewall protection provided by the Wireless Gateway is an intrinsic side effect of NAT (Network Address Translation). All users on the LAN share a single external IP address. From the external viewpoint, there is no network, only a single device.

For internal users, the Wireless Gateway acts as a “transparent proxy server”, translating the multiple internal IP addresses into a single external IP address.

For external requests, any attempt to connect to local resources is blocked. The Wireless Gateway will not “reverse translate” from a external IP address to a local IP address.

This type of “natural” firewall provides an impregnable barrier against malicious attacks.

## **Package Contents**

The following items should be included:

- The Wireless Gateway Unit
- Wireless PCMCIA Card
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual and Print Port Driver.

If any of the above items are damaged or missing, please contact your dealer immediately.

## **Physical Details**

### **Top-mounted LEDs**

<b>Power</b>	<b>On</b> - Power on. <b>Off</b> - No power.
<b>Status (Red)</b>	<b>On</b> - Error condition. <b>Off</b> - Normal operation. <b>Blinking</b> - This LED blinks during start up.
<b>WAN</b>	<b>On</b> - WAN connection is established. <b>Flashing</b> - Data is being transmitted or received via the WAN port.
<b>LAN: 10</b>	<b>On</b> - LAN connection is using 10BaseT. <b>Off</b> - No LAN connection. <b>Flashing</b> - Data is being transmitted or received via the LAN port.
<b>LAN: 100</b>	<b>On</b> - LAN connection is using 100BaseT. <b>Off</b> - No LAN connection. <b>Flashing</b> - Data is being transmitted or received via the LAN port.

<b>Wireless</b>	<b>On</b> - Wireless connection available; Wireless Access Point is ready for use. <b>Off</b> - No Wireless connection available. <b>Flashing</b> - Data is transmitted or received via the Wireless access point. This includes "network traffic" as well as user data.
<b>Print Error</b>	<b>On</b> - Printer error detected. <b>Off</b> - No printer error detected.
<b>Print Act</b>	<b>On</b> - Connection to printer established. <b>Off</b> - No connection to printer; printer is Off or Off-line. <b>Flashing</b> - Data is being transmitted to the printer.
<b>COM</b>	<b>Off</b> - Idle or no active device connected to the serial (RS232) port.
<b>(Serial Port)</b>	<b>Flashing</b> - Data is transmitted or received via the serial (RS232) port.

## Rear Panel

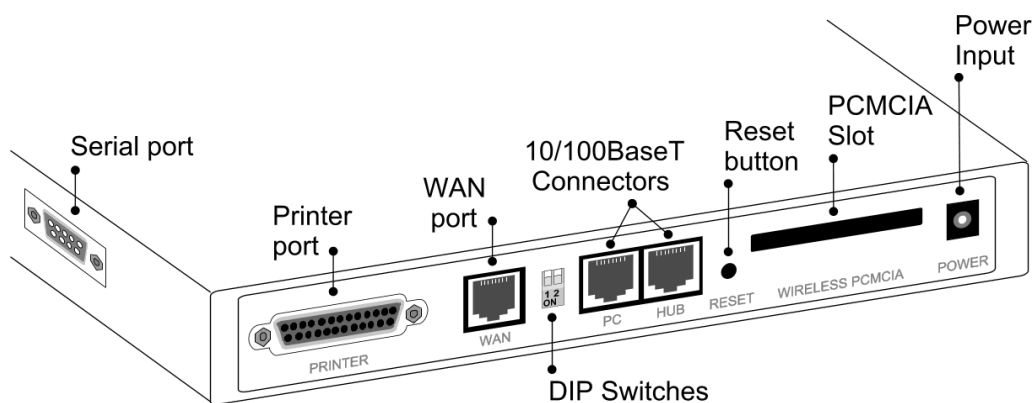


Figure 2: Rear Panel

<b>Serial Port</b>	RS232 Serial Port. If you have an analog modem or ISDN TA, connect it here.
<b>Printer Port</b>	Standard parallel printer port. If you wish to share a printer, connect it here.
<b>WAN port (10BaseT)</b>	Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.
<b>DIP switches</b>	Refer to the following table.
<b>PC port (10/100BaseT)</b>	If connecting directly to your PC (no Hub) use this port and a standard LAN cable (RJ45 connectors).  <b>Use EITHER the PC port OR the Hub port, NOT both.</b>
<b>HUB port (10/100BaseT)</b>	Use a standard LAN cable (RJ45 connectors) to connect this port to a 10BaseT or 100BaseT hub.  <b>Use EITHER the PC port OR the Hub port, NOT both.</b>



**Reset Button**

This button has three (3) functions:

- **Reboot.** When pressed and released, the Wireless Gateway will reboot (restart).
- **Diagnostic print-out.** If held down for 3 seconds, a diagnostic print-out will be sent to the attached printer.
  - Ensure the printer is ready.
  - Both *Print* LEDs will flash simultaneously during the diagnostic printing.
- **Clear All Data.** This button can also be used to clear ALL data and restore ALL settings to the factory default values.

**To Clear All Data and restore the factory default values:**

1. Power Off.
2. Hold the Reset Button down while you Power On.
3. Keep holding the Reset Button for a few seconds, until the RED LED has flashed TWICE.
4. Release the Reset Button. The Wireless Gateway is now using the factory default values.

**PCMCIA slot**





Insert the supplied Wireless PCMCIA card into this slot.

- ***Ensure the power is OFF before inserting or removing the PCMCIA Card.***
- ***Do not use any other PCMCIA Card.***

**Power port (12V)**

Connect the supplied power adapter here.

## DIP Switches

DIP Switch Setting	Description
 1=off 2=off	Normal Operation.
 1=off 2=on	DHCP Server function disabled.
 1=on 2=off	Used to restore Default IP Address and clear Password (See below).
 1=on 2=on	Normal Operation.

### Restore Default IP Address and Clear Password

If the Wireless Gateway's IP Address or password is lost, the following procedure can be used to recover from this situation.

- Turn the power to the Wireless Gateway OFF.
- Set DIP switch 1 ON.
- Turn the power to the Wireless Gateway ON.
- Operate DIP switch 1 in the following sequence (you have 15 seconds to complete the sequence):
  - OFF
  - ON
  - OFF
- The Wireless Gateway will now reset, and the Red Status LED flash. The following changes will have been made. (Other configuration data is unchanged.)
  - IP Address* set to its default value of 192.168.0.1
  - Network Mask* set to 255.255.255.0
  - DHCP Server* is enabled, and will allocate IP Addresses in the range 192.168.0.2 to 192.168.0.51.
  - The password cleared (no password).
- You can now connect to the Wireless Gateway and make any configuration changes required.

# Chapter 2

## Installation

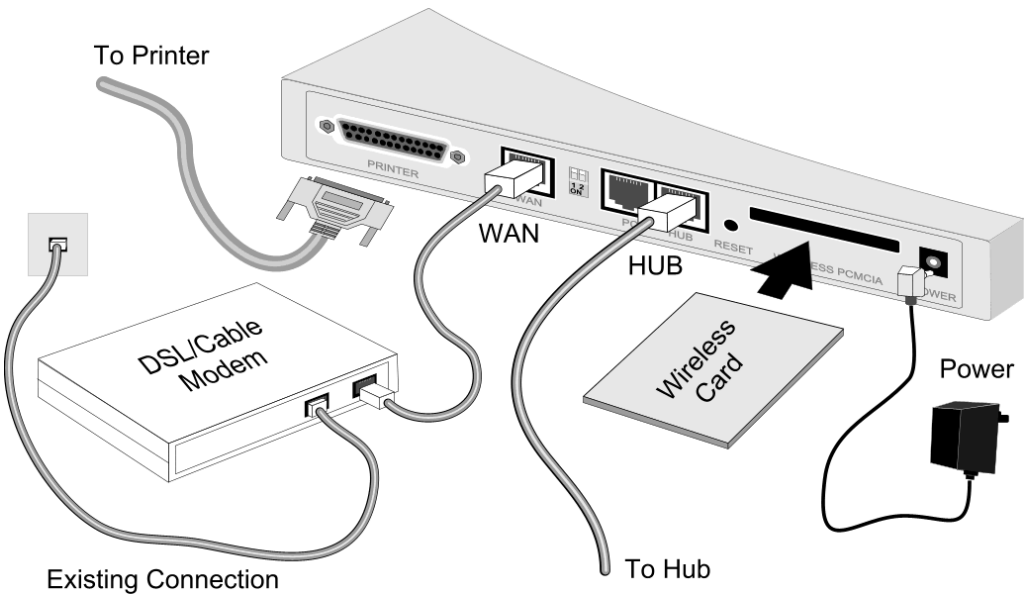
# 2

*This Chapter covers the physical installation of the Wireless Gateway.*

### Requirements

- Ethernet LAN (10/100BaseT) and the TCP/IP protocol.
- For Internet Access, an Internet Access account with an ISP, and either of:
  - A DSL or Cable modem (for WAN port usage)
  - An analog modem or ISDN TA (for serial port usage)
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE802.11b specifications.
- For shared access to the attached printer, the following clients are supported:
  - Windows 95/98/ME
  - Windows NT 4.0 or 2000
  - Apple Macintosh
  - Unix (LPD printing)

### Procedure



**Figure 3: Installation Diagram**

#### 1. Choose an Installation Site

Select a suitable physical location. Ensure the Wireless Gateway and the DSL/Cable modem are powered OFF.

## 2. Insert Wireless PCMCIA card

Ensuring the supplied Wireless PCMCIA card is the right way up, insert it into the slot on the rear. Push it firmly until it clicks into position.

## 3. Connect LAN Cable

Connect a standard LAN cable from a 10BaseT or 100BaseT Hub on your LAN to the “HUB” port on the Wireless Gateway.

## 4. Connect WAN Cable

If you have a DSL modem or Cable modem, connect it to the WAN port on the Wireless Gateway. Use the cable supplied with your modem. If no cable was supplied, use a standard LAN cable.

## 5. Connect Modem (optional)

If you wish to use an Analog modem or ISDN TA, use a standard serial cable to connect it to the Serial port on the Wireless Gateway.

## 6. Connect Printer Cable

Use a standard parallel printer cable to connect your printer to the Printer port on the Wireless Gateway.

## 7. Power Up

Connect the supplied power adapter and power up.  
**Use only the power adapter provided.**

## 8. Check the LEDs

- The *Status* LED should flash, then turn Off. If it stays on, there is a hardware error.
- The *Power* LED should be ON.
- One (1) of the LAN LEDs (*10* or *100*) should be ON.
- The *Wireless* LED should be ON.
- If the printer is On and On-line, the *Print Act* LED should be ON.

For more information, refer to Top-mounted LEDs in Chapter 1.

# Chapter 3

## Configuration



*This Chapter provides details of the configuration process.*

### Overview

This chapter describes the procedure for:

- Quick setup
- Wireless access point configuration
- Using the Status screens

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*.

Other configuration may also be required, depending on which features and functions of the Wireless Gateway you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Configure PCs on your LAN.	Chapter 4: PC Configuration
Learn more about using DHCP on the internal LAN.	Chapter 5: DHCP
Configure and use the Serial (RS232) port, either for Internet access or for Dial-in.	Chapter 6: Serial Port
Configure various options: <ul style="list-style-type: none"><li>• Set a password for the Wireless Gateway, to protect the configuration data.</li><li>• Disable NAT (Network Address Translation),</li><li>• Enable TFTP firmware upgrade feature.</li><li>• Configure Remote Management (configure via the Internet)</li><li>• Access the Printer Port setup screen.</li></ul>	Chapter 7: Options
Configure the Wireless Gateway and other routers for a LAN which already has 1 or more routers.	Chapter 8: Routing
Use any of the following features: <ul style="list-style-type: none"><li>• Special Internet Applications</li><li>• URL Filter</li><li>• Virtual Servers</li><li>• DMZ</li></ul>	Chapter 9: Advanced Internet Features
Limit Internet Access by individual workstations.	Chapter 10: Access Control



Where use of a certain feature requires that PCs or other LAN devices be configured, this is also explained in the relevant chapter.

## Configuration Program

The Wireless Gateway contains an HTTP server. This enables you to connect to it, and configure it, using your Web Browser.

Most Browsers should work, provided they support HTML tables and forms.

### Preparation

Before attempting to configure the Wireless Gateway, please ensure that:

- Your PC can establish a physical connection to the Wireless Gateway. The PC and the Wireless Gateway must be directly connected (using the “PC” port on the Wireless Gateway) or on the same LAN segment.
- The Wireless Gateway must be installed and powered ON.
- If the Wireless Gateway's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the Wireless Gateway is allocated a new IP Address during configuration.

### Connecting to the Wireless Gateway

To establish a connection from your PC to the device:

1. After installing the Wireless Gateway in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the Wireless Gateway, as in this example, which uses the Wireless Gateway's default IP Address:  
`HTTP://192.168.0.1`
4. You should then see the *Quick Setup* screen.  
See the following section for details on using this screen.

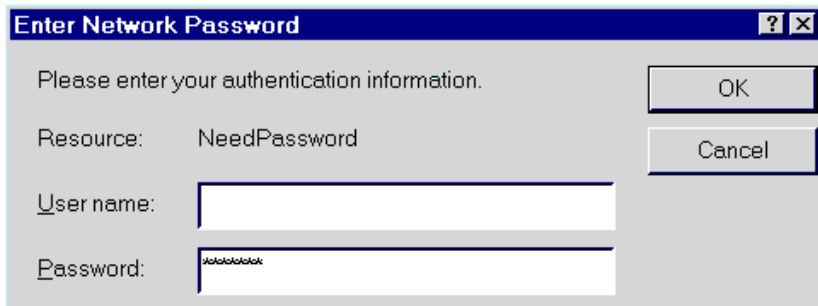
#### If you can't connect

If the Wireless Gateway does not respond, check the following:

- The Wireless Gateway is properly installed, LAN connection is OK, and it is powered ON.
- Ensure that your PC and the Wireless Gateway are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the Wireless Gateway's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 – PC Configuration* for details on checking your PC's TCP/IP settings.

## Password

If you have assigned a password to the Wireless Gateway (on the *Options* screen) you will be prompted for the password, as shown below. (If no password has been set, this dialog will not appear.)



Enter Network Password

Please enter your authentication information.

Resource: NeedPassword

User name:

Password:

OK

Cancel

**Figure 4: Password Dialog**

- Leave the "User Name" blank.
- Enter the password for the Wireless Gateway, as set on the *Options* screen.

## Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must "Save" before changing screens or your data will be ignored.



**Note!**

**On each screen, clicking the "Help" icon will display help for that screen.**

## Quick Setup Screen

The *Quick Setup* screen, like the example below, will be displayed when you first connect.

MILAN TECHNOLOGY		ShAir Office™ wireless gateway	
<input type="button" value="Help"/>			
<b>Router</b>	Device(Host) Name: <input type="text" value="SO220000"/>		
	Hardware (MAC) Address: <b>00-40-c8-22-00-00</b>		
<b>LAN</b>	Device IP Address: <input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="0"/> <input type="text" value="1"/>		
	Network Mask: <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>		
	<input checked="" type="checkbox"/> DHCP Server Start IP Address: <input type="text" value="-"/> <input type="text" value="-"/> <input type="text" value="-"/> <input type="text" value="2"/>		
	Finish IP Address: <input type="text" value="-"/> <input type="text" value="-"/> <input type="text" value="-"/> <input type="text" value="51"/>		
<b>WAN</b>	<input checked="" type="checkbox"/> Enable Ethernet port		
	IP Address from ISP: <input checked="" type="radio"/> Dynamic IP Address		
	<input type="radio"/> Fixed IP Address		
	IP Address <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
	Network Mask <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
	Gateway <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
	DNS <input type="text" value="168"/> <input type="text" value="95"/> <input type="text" value="192"/> <input type="text" value="1"/>		
	Mask & Gateway are not required for PPPoE		
	<input type="checkbox"/> PPPoE (PPP Over Ethernet)		
	Account/User Name <input type="text" value="guest"/>		
	Password <input type="text"/> Verify: <input type="text"/>		
	<input type="checkbox"/> Connect On Demand		
	<input type="checkbox"/> Disconnect after idle for <input type="text" value="15"/> minutes		
<b>Wireless</b>	SSID (Service Set Identifier): <input type="text" value="default"/>		
	WEP Status: Disabled		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>			

**Figure 5: Quick Setup Screen**

## Quick Setup - Overview

This screen contains all the basic data to make the Wireless Gateway operational.

For many users, the default values will be satisfactory, and no changes will be required.

- **Router** Most users do not need to change these values.
- **LAN Settings** There is no need to change the LAN settings unless:
  - You wish to use a different IP Address range
  - You already have a DHCP Server or a Router on your LAN.  
See *Chapter 5 -DHCP* for more details about DHCP, or *Chapter 8 - Routing* for details about using Routers on your LAN.
- **WAN Port Settings** By default, the Wireless Gateway is configured for WAN access using a "Direct Connection" (cable modem or permanent DSL link) and a dynamic IP Address (the IP Address is supplied by your ISP when you connect). For this common situation, no changes are required.



- **Wireless Access Point** To use the Wireless Access Point:
  - All Wireless devices must have the same SSID. Either the Wireless Access Point or the Wireless clients can be changed to ensure this.
  - All Wireless devices must have the same settings for WEP (Wired Equivalent Privacy).  
By default, WEP on the Wireless Gateway is **Disabled**, so clients also need to have WEP **Disabled**.
  - See Appendix B for more details about Wireless LANs and WEP, and the *Wireless Screen* section later in this chapter for details of the Wireless Gateway's *Wireless* screen.

## Configuration Data - Quick Setup Screen

Router	
<b>Device (Host) Name</b>	Normally, there is no need to change the default name, but if your ISP requests that you use a particular "Hostname", enter it here. This name will be provided to, and recorded by, the remote DHCP Server.
<b>Hardware (MAC) Address</b>	Also called <i>Network Adapter Address</i> or <i>Physical Address</i> . This is a low-level identifier for the Wireless Gateway, as seen from the WAN port.  Provide this value to your ISP if requested. If you did not provide this value when first connected, there is no need to provide it now.
LAN	
<b>Device IP Address</b>	IP address for the Wireless Gateway, as seen from the local LAN. Use the default value of 192.168.0.1 unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
<b>Network Mask</b>	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Network Mask for the LAN segment to which the Wireless Gateway is attached. i.e. the same value as the PCs on that LAN segment.
<b>DHCP Server</b>	See Chapter 5 for further details about DHCP. <ul style="list-style-type: none"> <li>• If <b>Enabled</b>, the Wireless Gateway will allocate IP Addresses to PCs on your LAN. The default and recommended value is <b>Enabled</b>.</li> <li>• If you are already using a DHCP Server, this setting must be <b>DISABLED</b>, and the existing DHCP server must be re-configured as described in <i>Chapter 5 - DHCP</i>.</li> <li>• The <b>Start IP Address</b> and <b>Finish IP Address</b> fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. (Maximum 253.)</li> </ul>

<b>WAN</b>	
<b>Enable Ethernet Port</b>	<p>Normally, this should be left at the default value of <b>Enabled</b>.</p> <ul style="list-style-type: none"> <li>• If no DSL or Cable modem is connected to the WAN (Ethernet) port, then this setting should be Disabled.</li> <li>• If Internet access via the Serial Port is Enabled, this setting will be automatically Disabled. It is not possible to simultaneously use both the WAN (Ethernet) port and the Serial (RS232) port for Internet access.</li> </ul>
<b>IP Address from ISP</b>	<p><b>Dynamic IP Address.</b> This is the default, and the most common. Leave this selected if your ISP allocates an IP Address to the Wireless Gateway upon connection.</p> <p><b>Fixed IP Address.</b> Select this if your ISP has allocated you a fixed IP Address. If this option is selected, the following data must be entered.</p> <ul style="list-style-type: none"> <li>• <b>IP Address.</b> The IP Address allocated by the ISP.</li> <li>• <b>Network Mask (Not required for PPPoE)</b> This is also supplied by your ISP. It must be compatible with the IP Address above.</li> <li>• <b>Gateway IP Address (Not required for PPPoE)</b> The address of the Gateway or gateway, as supplied by your ISP.</li> <li>• <b>DNS IP Address</b> The DNS (Domain Name Server) IP Address provided by your ISP. If required, additional DNS entries can be made on the <i>Options</i> screen.</li> </ul>
<b>PPPoE</b>	<p>If your ISP uses PPPoE, enable this checkbox and enter the data in the <i>PPPoE</i> section, as described below.</p> <p>If your ISP's data does not mention "PPPoE", do NOT enable this option.</p>
Account/User Name	The "Login" name, or the name of the Internet account provided by your ISP.
Password and Verify	Enter the password for the above account. Re-enter the password in the <i>Verify</i> field, to ensure it is correct.
Connect on Demand	<p>Normally, this should be Enabled.</p> <p>If disabled, you must use the <i>Connect</i> button on the <b>Status</b> screen to establish a connection.</p>
Disconnect after Idle	<p>Enable this if you wish an idle connection to be terminated.</p> <p>If enabled, enter the idle time-out period (in minutes) in the field provided. After the connection to your ISP has been idle for this time period, the connection will be terminated.</p>
<b>Wireless</b>	
<b>SSID (Service Set Identifier)</b>	<p>To communicate, all Wireless stations MUST use the same SSID/ESSID. You can either change this value, or change your client Wireless stations, to ensure this.</p> <p>The default SSID value for the Wireless Gateway is <b>default</b>.</p> <p><b>Note! The SSID is case sensitive.</b></p>

<b>WEP Status</b>	This will state "Enabled" or "Disabled". The default is "Disabled". <ul style="list-style-type: none"><li>• In order to use the Wireless Gateway's access point, the client wireless stations must have the same settings for WEP.</li><li>• To change the Wireless Gateway's WEP settings, use the <i>Wireless</i> screen, described in the following section.</li></ul>
<b>Buttons</b>	
<b>Save</b>	Save any data you have entered on this screen. Remember to save before changing to another screen.
<b>Cancel</b>	Cancel any changes you have made since the last "Save" operation.

Once this screen is completed, the Wireless Gateway is ready for use.

- If you wish to use WEP, or change other Wireless Access Point settings, refer to the following section.
- Your PCs may require configuration. Refer to *Chapter 4 - PC Configuration* for details.
- To check the status of the Wireless Gateway, and confirm that it is working correctly, refer to the *Status Screen* section later in this Chapter.

## Wireless Screen

The Wireless Access Point settings must match the other Wireless stations. To change the Wireless Gateway's default settings for the Wireless Access Point, use the *Wireless* link on the main menu to reach the *Wireless* screen. An example screen is shown below.

**MILAN TECHNOLOGY** **ShAir Office™** wireless gateway

**Configuration**

Regulatory Domain: USA/Canada  
 Station Name: S0220000  
 SSID (Service Set Identifier): ANY  
 Channel No: 10

**WEP Data Privacy**

Off - no data encryption  
 64 Bit Encryption using this key table  
 128 Bit Encryption using this key

Default Key: 1

Key 1: 00 00 00 00 00  
 Key 2: 00 00 00 00 00  
 Key 3: 00 00 00 00 00  
 Key 4: 00 00 00 00 00

WEP Authentication: Shared Key

**Wireless Station Access**

Enable Wireless Access Point

Wireless Stations: [Empty List] [Delete]

New Station Address: [Empty Field] [Add]

**Access Permission**

For Wireless Stations listed above:  Allow Internet access  
 Allow LAN access

For Other Wireless Stations:  Allow Internet access  
 Allow LAN access

[Save] [Cancel]

Figure 6: Wireless Screen

### Data – Wireless Screen

Configuration	
<b>Regulatory Domain</b>	It is illegal to use this device in any location outside of the regulatory domain.
<b>Station name</b>	This is the same as the <i>Device (Host) Name</i> on the WAN screen. On your PC, some Wireless status screens may display this name as the Access Point in use.

<b>SSID (ESSID)</b>	To communicate, all Wireless stations <b>MUST</b> use the same SSID/ESSID. The default value is <b>default</b>  <b>Note! The SSID is case sensitive.</b>
<b>Channel No.</b>	Select the value you wish to use on your Wireless LAN. If you experience lost connections and/or slow data transfers you may need to experiment with different channels to see which is the best.
<b>WEP Data Privacy</b>	
<b>Off</b>	If OFF (default), data is NOT encrypted before being transmitted.
<b>64 Bit Encryption</b>	<ul style="list-style-type: none"> <li>If selected, data is encrypted, using the default key, before being transmitted. The receiving station must be set to 64 Bit Encryption, and have the same Key value in the same position in its key table. Otherwise, it will not be able to decrypt the data.</li> <li><b>Default Key</b> Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only.</li> <li><b>Key Table</b> <ul style="list-style-type: none"> <li>This table is used when Encrypting and Decrypting data. All stations, including this Access Point, always transmit data encrypted using their default key. The key number (1, 2, 3, 4) is also transmitted. The receiving station will use the key number (1, 2, 3, 4) to determine which key value to use for decryption. If the key value does not match the transmitting station, decryption will fail.</li> <li>The easiest way to ensure there are no problems is to have every Station, including the Access Point, use the same key table (all entries identical). Then, it does not matter which key is used as the default key.</li> </ul> </li> </ul>
<b>128 Bit Encryption</b>	<ul style="list-style-type: none"> <li>If selected, data is encrypted using the key before being transmitted. The receiving station must be set to use 128 Bit Encryption, and have the same Key value. Otherwise, it will not be able to decrypt the data.</li> <li><b>Key</b> Enter the key value you wish to use. Other stations must have the same key.</li> </ul>
<b>WEP Authentication</b>	Select the appropriate value - "Open System" or "Shared Key". Check your Wireless card's documentation to see what method to use. Some Wireless cards do not support both methods.
<b>Wireless Station Access</b>	
<b>Enable Wireless Access Point</b>	<ul style="list-style-type: none"> <li>If enabled (default), this device can act as a Wireless Access Point.</li> <li>If not enabled, no Wireless stations can use this device as a Wireless Access Point.</li> </ul>

<b>Existing Stations</b>	<ul style="list-style-type: none"> <li>• This lists the Wireless stations you have entered. If you have not entered any stations, this list will be empty.</li> <li>• To delete an entry, select it, and click the "Delete" button. Multiple entries may be selected by hold down the CTRL key while selecting. (On the Macintosh, use SHIFT instead of CTRL.)</li> </ul>
<b>New station Address</b>	<ul style="list-style-type: none"> <li>• Use this field to add a new station to the list. Just enter its address here, and click the "Add" button.</li> <li>• Use the software supplied with your Wireless unit to determine its address. The address consists of 12 letters (A..F) and digits (0..9) like this example:  10F810A81091   The address may be shown with separators ( : or - ) between each pair of characters.  Do NOT enter the separators ( : or - ) in this field.</li> </ul>
<b>Access Permission</b>	<ul style="list-style-type: none"> <li>• <b>For Wireless Stations listed above</b>  This setting determines what type of access is available to Wireless stations whose address has been entered in the "Wireless Stations" list.</li> <li>• <b>For Other Wireless Stations</b>  This setting determines what type of access is available to Wireless stations whose address is NOT in the "Wireless Stations" list.</li> <li>• For either category, if neither "Internet" nor "LAN" access is enabled, Wireless stations are unable to use this Access Point.</li> </ul>
<b>Buttons</b>	
<b>Delete</b>	<b>Delete</b> will delete the selected entry or entries in the list.
<b>Add</b>	<b>Add</b> will add the <i>New Station</i> data to the list.
<b>Save</b>	<b>Save</b> will save the other data on the screen. This has no effect on the contents of the <i>Wireless Stations</i> list.

## Status Screen

Use the *Status* link on the main menu to view this screen.

The *LAN Status* link on the menu will result in a screen like the example below.

MILAN TECHNOLOGY		ShAir Office™ wireless gateway	
<a href="#">Help</a>			
<b>LAN</b>	Device Name:	SO220000	
	IP Address:	199.86.12.9	
	Network Mask:	255.255.255.0	
	Physical (Hardware) Address:	00-40-c8-22-00-00	
	DHCP Server:	Enable	
	<b><u>DHCP Table</u></b>	IP Addresses allocated by the DHCP Server function.	
<b>System</b>	Firmware Version:	Version 1.1 Release 01	
	Printer Status:	Off Line	
	System Data		
	<div style="border: 1px solid gray; height: 80px;"></div>		
<b>WAN</b>	<b><u>WAN (Ethernet) Port</u></b>	View current connection status.	
	<b><u>Serial Port</u></b>	Check serial port usage.	
	<b><u>Access Control Log</u></b>	Attempted connections which have been blocked by the Access Control feature.	
	<b><u>Internet Access Log</u></b>	Details of outgoing connections to the Internet.	
<a href="#">Refresh</a>			

Figure 7: Status Screen

### Data - Status Screen

LAN	
<b>Device Name</b>	This shows the name of the device.
<b>IP Address</b>	The IP Address of this device, as seen by other devices on the Internal LAN.
<b>Network Mask</b>	The Network Mask (Subnet Mask) for the IP Address above.
<b>Physical Address</b>	The "Hardware" address of this device, as seen by other devices on the Internal LAN.
<b>DHCP Server</b>	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".

<b>DHCP Table</b>	<p>Use this link to view the IP Addresses which have been allocated to LAN devices, or the Dial-in user, by the DHCP Server function.</p> <p>The DHCP Table contains the following data:</p> <ul style="list-style-type: none"> <li>• <b>Port</b> - The port which the DHCP client used to access this device. Possible values are LAN, WLAN (Wireless LAN), and RS232 (serial port).</li> <li>• <b>IP Address</b> - The IP Address which has been allocated by the DHCP server to the DHCP client.</li> <li>• <b>Physical (Hardware) Address</b> - The Physical Address (Hardware Address) of the DHCP client which has been allocated this IP Address.</li> <li>• <b>Status</b> - Possible Status values are "Leased" (the IP Address is allocated to the device shown) or "Reserved" (the IP Address is reserved for this device, but not currently allocated).</li> </ul> <p>"Reserved" entries are generated for the Dial-in User, and for any PCs for which an IP Address has been reserved. An IP Address can be reserved for a particular PC using the <i>Access Control - PCs</i> screen. The <i>Access Control</i> feature is described in Chapter 10.</p>
<b>System</b>	
<b>System Data</b>	This is identical to the data shown on a "Diagnostic Printout", and contains all system information.
<b>Firmware Version</b>	The version of the firmware currently installed in this device.
<b>Printer Status</b>	This shows the status of the printer. Click the "Refresh Screen" button to update this information.
<b>WAN Links</b>	
<b>WAN (Ethernet) Port</b>	<p>View the WAN (Ethernet) status screen. This screen will vary according to the connection method used (Direct connection or PPPoE).</p> <p>See the following sections <i>WAN Status - Direct Connection</i> and <i>WAN Status - PPPoE</i> for details.</p>
<b>Serial Port</b>	Check the status of the Serial Port. This screen is also accessible from the <i>Serial Port</i> sub-menu. See <i>Chapter 6 - Serial Port</i> for details of this screen.
<b>Access Control Log</b>	View details of connection attempts which have been blocked. See below for more information.
<b>Internet Access Log</b>	View details of outgoing connections to the internet. See below for more information.



## Access Control Log

This log shows connection requests which have been blocked by the *Access Control* feature or the built-in NAT Firewall.

Accesses which have been blocked for other reasons (e.g. URL filter, incorrect dial-in password, incorrect WEP settings on the WLAN) are NOT shown in this log. (The "Internet Access Log" can be used to view connection attempts which have been blocked by the URL filter.)

Data shown in this log is as follows:

- **Port** - The port used to gain access to this device. Possible values are LAN, WAN, WLAN (Wireless LAN), and RS232 (serial port).
- **Source IP Address** - The IP Address of the PC or device whose access request was blocked.
- **Physical Address (Hardware Address)** - The hardware address of the PC or device whose access request was blocked.
- **Name** - If known, the name of the device whose access was blocked. This name is taken from the *Access Control* database. For Wireless devices, the name is obtained from the *Wireless Stations* list, and so will always match the Physical (Hardware) address.
- **Destination** - The destination of the attempted access. Possible values are "Internet", "LAN" or "WLAN".
  - "Internet" indicates an attempt by a LAN user, WLAN user, or dial-in user to access the Internet using a protocol and/or port number which was blocked.
  - "LAN" or "WLAN" indicates a connection attempt from the Internet which was not allowed. The protocol (TCP or UDP) and port number are shown in braces.

This data is useful if you want the access to be allowed. In this case, you can use this data to configure the *Advanced Internet - User-defined Virtual Servers* screen or the *Advanced Internet - Special Applications* screen. (In the case of a Special Application, this log indicates the "Incoming Connection" for the Special Application.)

See *Chapter 9 - Advanced Internet* for further details of the *Virtual Server* and *Special Applications* features.

## Internet Access Log

This log shows details of Internet access by LAN users, WLAN users, or the dial-in user.

Details shown in this log are as follows:

- **Source IP Address** - The IP Address of the LAN user, WLAN user, or dial-in user making the connection request.
- **Destination** - The requested Internet IP Address or URL. Normally, the IP Address will be shown. But if the *URL Filter* feature is Enabled, the URL will be displayed. For details on using the *URL Filter*, refer to *Chapter 9 - Advanced Internet*.
- **Blocked** - This will indicate "Yes" if the connection attempt was blocked by the URL Filter. Otherwise, this will be blank.

## WAN Status – Direct Connection

If the WAN (Ethernet) port is using PPPoE, then clicking the *WAN Status* link on the *Status* screen will reveal a screen like the following.



**Figure 8: WAN Status – Direct Connection**

### Data

WAN Status	
<b>Physical Address</b>	The "Hardware" address of this device, as seen by other devices on the WAN.
<b>IP Address</b>	The IP Address of this device, as seen by devices on the WAN. (This device has 2 IP Addresses; one for the local LAN, and another for the WAN port.)
<b>Network Mask</b>	The Network Mask for the above IP Address.
<b>Default Gateway</b>	IP address of the Router/Gateway on the WAN port.
<b>DHCP Client</b>	Displays "Enabled" or "Disabled", indicating whether this device is acting as a DHCP client on the external LAN or WAN.
Buttons	
<b>Reconnect</b>	Use this button if the connection seems to have been lost, and no data is being transferred. (This button has no effect unless acting as a DHCP Client.)
<b>Refresh</b>	Update the data on screen.

## WAN Status – PPPoE

If the WAN (Ethernet) port is using PPPoE, then clicking the *WAN Status* link on the *Status* screen will reveal a screen like the following.

Figure 9: WAN Status – PPPoE

### Status Data

WAN Status	
<b>Physical Address</b>	The "Hardware" address of this device, as seen by other devices on the WAN.
<b>IP Address</b>	The IP Address of this device, as seen by devices on the WAN. (This device has 2 IP Addresses; one for the local LAN, and another for the WAN port.)
<b>Network Mask</b>	The Network Mask (Subnet Mask) for the IP Address above.
<b>PPPoE Link Status</b>	This indicates whether or not the connection is currently established. If the connection does not exist, the <b>Connect</b> button can be used to establish a connection. If the connection currently exists, the <b>Disconnect</b> button can be used to break the connection.
Connection Log	
<b>Log Data</b>	This shows status messages relating to the existing connection. The most common messages are listed in the following table.

<b>Buttons</b>	
<b>Connect</b> <b>Disconnect</b> <b>N/A</b>	<p>If not connected, this button will display "Connect" and can be used to establish a connection to your ISP</p> <p>If connected to your ISP, this button will display "Disconnect" and can be used to hang up the connection.</p> <p>If PPPoE is not configured, this button will display "N/A" (not applicable).</p>
<b>Clear Log</b>	Delete all data currently in the Log. This will make it easier to read new messages.
<b>Refresh</b>	Contact this device and update the Log data.

## Connection Log Messages

<b>Message</b>	<b>Description</b>
Connect on Demand	Connection attempt has been triggered by the "Connect on Demand" setting.
Manual connection	Connection attempt started by the "Connect" button.
Reset physical connection	Preparing line for connection attempt.
Connecting to remote server	Attempting to connect to the ISP's server.
Remote Server located	ISP's Server has responded to connection attempt.
Start PPP	Attempting to login to ISP's Server and establish a PPP connection.
PPP up successfully	Able to login to ISP's Server and establish a PPP connection.
Idle time-out reached	The connection has been idle for the time period specified in the "Idle Time-out" field. The connection will now be terminated.
Disconnecting	The current connection is being terminated, due to either the "Idle Time-out" above, or "Disconnect" button being clicked.
Error: Remote Server not found	ISP's Server did not respond. This could be a Server problem, or a problem with the link to the Server.
Error: PPP Connection failed	Unable to establish a PPP connection with the ISP's Server. This could be a login problem (name or password) or a Server problem.
Error: Connection to Server lost	The existing connection has been lost. This could be caused by a power failure, a link failure, or Server failure.
Error: Invalid or unknown packet type	The data received from the ISP's Server could not be processed. This could be caused by data corruption (from a bad link), or the Server using a protocol which is not supported by this device.

# Chapter 4

## PC Configuration



*This Chapter details the PC Configuration required on the local ("Internal") LAN.*

### Overview

For each PC, the following may to be configured:

- TCP/IP network settings
- Internet Access configuration
- Network printer
- Wireless configuration

### Windows Clients

This section describes how to configure Windows clients for:

- Internet access via the Wireless Gateway
- Printing using the printer attached to the Wireless Gateway.
- Remote Dial-in access to the modem attached to the Wireless Gateway's serial (RS232) port.

The first step is to check the PC's TCP/IP settings.

The Wireless Gateway uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

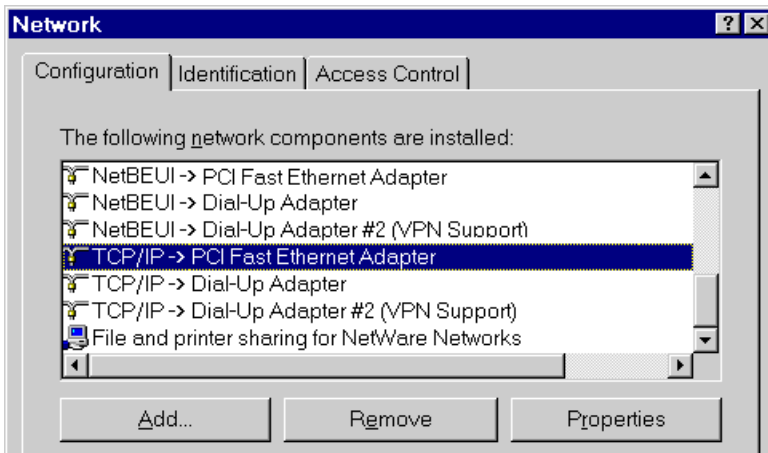
### TCP/IP Settings

**If using the default Wireless Gateway settings, and the default Windows 95/98 TCP/IP settings, no changes need to be made.**

- By default, the Wireless Gateway will act as a DHCP Server, automatically providing a suitable IP Address to each PC when the PC boots.
- The default Windows 95/98 TCP/IP setting is to act as a DHCP client.

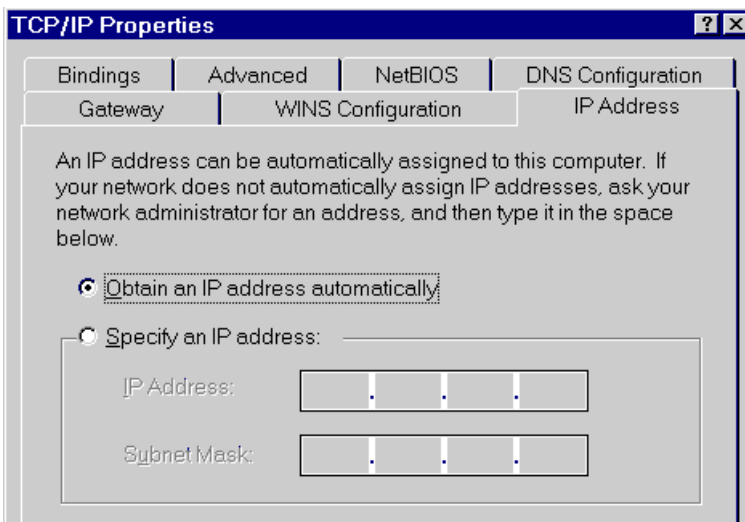
#### **To check your PC's TCP/IP Settings:**

1. Select *Control Panel - Network*. You should see a screen like the following:



**Figure 10: Network Configuration**

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.



**Figure 11: IP Address (Win 95)**

Ensure your TCP/IP settings are correct, as follows:

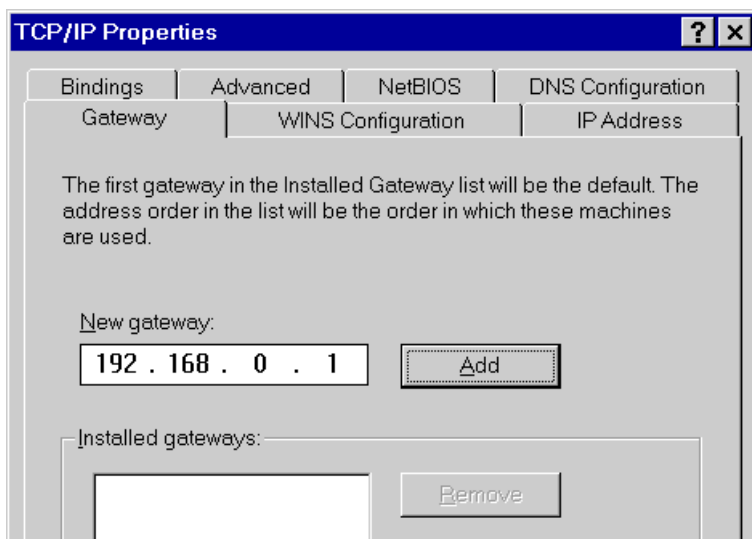
### Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the Wireless Gateway.

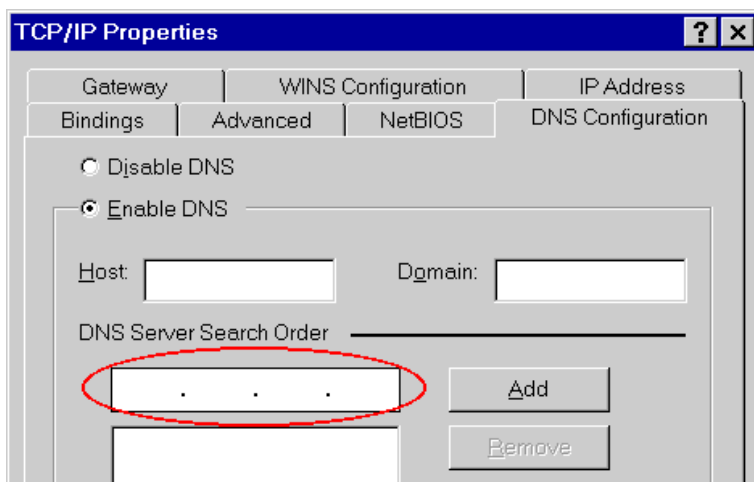
### Using “Specify an IP Address”

- If your PC is already configured, do NOT change the settings on the IP Address tab shown in Figure 11 above.
- On the *Gateway* tab, enter the Wireless Gateway's IP address in the *New Gateway* field and click *Add*. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Gateway.



**Figure 12: Gateway Tab (Win 95/98)**

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.



**Figure 13: DNS Tab (Win 95/98)**



**Note!**

If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to *Chapter 8 - Routing* for details.

---

## Internet Access

If you are using the Wireless Gateway for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
  - Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.
1. Select *Start Menu - Settings - Control Panel - Internet Options*.
  2. Select the *Connection* tab, and click the *Setup* button.
  3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click "Next".
  4. Select "I connect through a local area network (LAN)" and click "Next".
  5. Ensure all of the boxes on the following *Local area network Internet Configuration* screen are **unchecked**.
  6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?".
  7. Click "Finish" to close the Internet Connection Wizard.
  8. Then simply use your Browser, FTP client, or other Internet client to connect to the desired Internet site.

## Accessing AOL

To access AOL (America On Line) through the Wireless Gateway, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "Wireless Gateway".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.  
Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "Wireless Gateway" location.



## Printing Setup

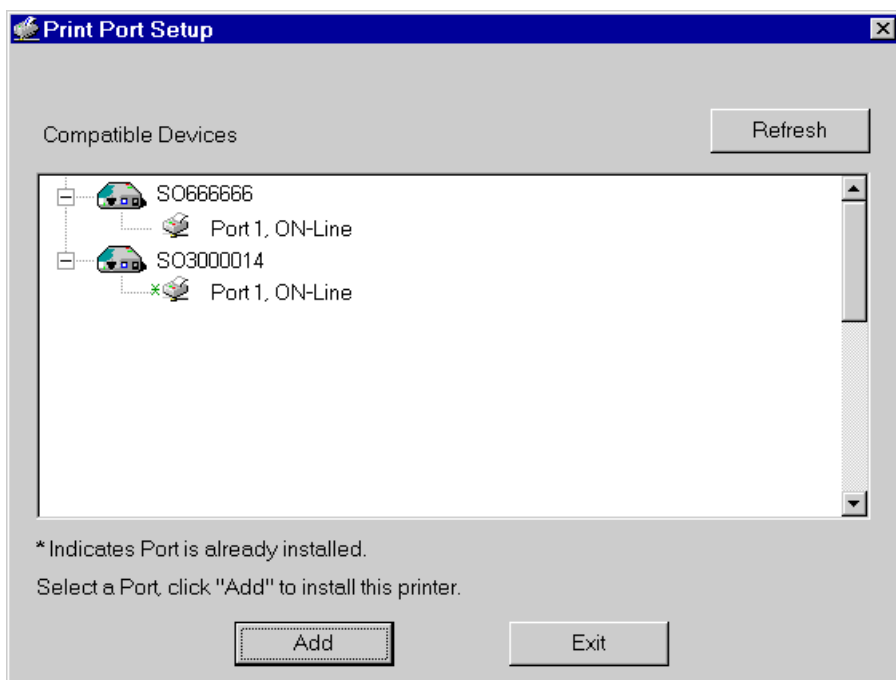
The Wireless Gateway provides printing support for 2 methods of printing from Windows:

- **Print Port Driver.** After installing the Print Port Driver, Windows users can print directly to the Wireless Gateway. Print jobs are spooled (queued) on each PC. The supplied Print Port Driver supports Windows 95/98, Windows ME, Windows NT4.0, and Windows 2000.
- **LPD/LPR Printing.** If using Windows NT 4.0 Server or Windows 2000 Server, LPD/LPR printing can be used. No software needs to be installed on either the Windows Server or each client PC. Print jobs will be spooled (queued) on the Windows Server, and can be managed using the standard Windows Server tools.

### Print Port Driver Setup

The following procedure is for Windows 95/98, Windows ME, Windows NT4.0, and Windows 2000.

1. Insert the supplied CD-ROM into your drive. If the setup program does not start automatically, run SETUP.EXE in the root folder.
2. At the *Setup Type* screen, select the correct model.
3. At the *Select Components* screen, select the **Print Port Driver** option.
4. Follow the prompts to complete the installation.
5. The *Print Port Setup* will then run, and the following screen will be displayed.

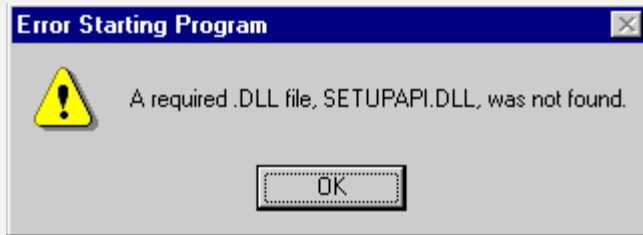


**Figure 14: Print Port Setup**

6. Select the desired device and port, and then click the "Add" button.



If you see the following error message, either install Internet Explorer 4 or later, or follow the procedure in the "Trouble Shooting - Printing" section of Appendix A.



7. A pop-up message will inform you if the port has been created successfully, and then the Windows *Add Printer* wizard will start.
  - Select the correct Printer Manufacturer and Model, or use the "Have Disk" option if appropriate.
  - If desired, change the Printer name so it indicates the device used (e.g. HP2100 on SCA43600)
  - If prompted about Sharing, do NOT enable Sharing.
8. Installation is now complete. You can now print using this printer.
  - To install additional Printers, repeat steps 6 and 7.
  - Use the **Start** menu to run this program in future. The default installation is *Start - Programs - Broadband Internet Router - Add Port*.

## Management

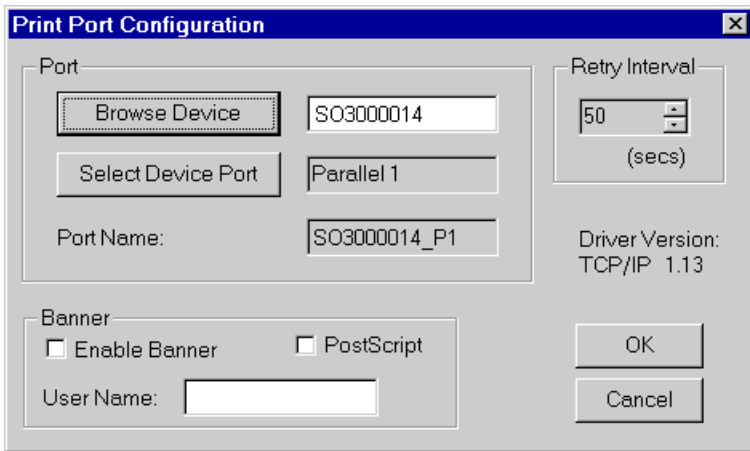
- Print jobs can be managed like any Windows printer. Open the *Printers* folder (*Start - Settings - Printers*) and double-click any printer to see the current print jobs.
- If the printer attached to the Wireless Gateway is changed, just run this program again, and select the correct printer.
- To delete a port created by this setup program, use the Windows *Delete Port* facility:
  - Right-click any printer in the *Printers* folder, and select *Properties*.
  - Locate the *Delete Port* button. This button is on the *Details* or *Ports* tab, depending on your version of Windows.
- If the Wireless Gateway's IP Address is changed, and you can no longer print, delete the port (see procedure above) and re-install it.

## Port Options

The options for the *Print Port Driver* are accessed via the Windows *Port Settings* button.

Use *Start - Settings - Printers* to open the *Printers* folder, then right-click the Printer, and select *Properties*. The *Port Settings* button is on the *Details* or *Port* tab, depending on your version of Windows.

An example screen is shown below:



**Figure 15: Print Port Configuration**

Items shown on this screen are as follows:

<b>Port</b>	If desired, click <i>Browse</i> to select a different device. (The <i>Select Device Port</i> button is provided to allow this software to work with multi-port models.) The <i>Port Name</i> is shown in the Printer's <i>Properties</i> .
<b>Banner</b>	Check this option to print a banner page before each print job. <ul style="list-style-type: none"> <li>• If using a PostScript Printer, check the <i>PostScript</i> box.</li> <li>• The <i>User Name</i> will be printed on the banner page.</li> </ul>
<b>Retry Interval</b>	Sets how often Windows will poll the Wireless Gateway to establish a connection when the printer is busy. Increase this value if you get too many warning messages.

## LPD/LPR Printing

LPD/LPR printing can be used with Windows NT 4.0 Server or Windows 2000. No software needs to be installed.

### Windows NT 4.0 Server Configuration

To use LPD printing, **Microsoft TCP/IP Printing** must be installed and enabled. This can be checked using *Start-Settings-Control Panel-Network - Services*.

To install LPD printing using the Wireless Gateway, follow this procedure:

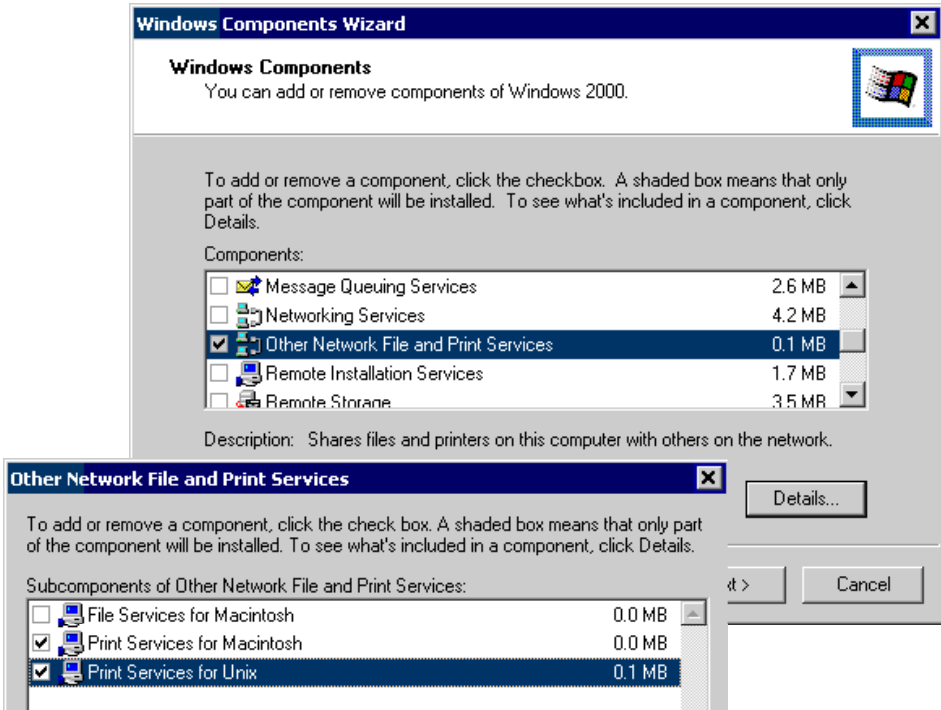
1. Go to *Start-Settings-Printer* and invoke the *Add Printer* wizard.
2. When prompted with "This printer will be managed by..", select **My Computer** and click **Next**.
3. Select **Add Port...**, then select **LPR Port** and click **New Port**.
4. In the Dialog requesting *Name of Address of server providing lpd*, enter the IP address of the Wireless Gateway.
5. For *Name of printer or print queue on that server*, enter L1
6. Click **OK**. When returned to the Printer Ports window, simply select *Close* and then install your printer driver as usual.
7. When prompted whether or not the printer will be shared, select the **Sharing** radio button.

8. In the *Shared* dialog box, enter the shared printer name. The shared name is how other users will see this printer. You should advise client PCs of the Server name and this printer name.
9. Click OK to save and exit.

## Windows 2000 Server Configuration

The *LPD/LPR Port* is not enabled by default. To enable it, use this procedure:

1. In *Control Panel*, select *Add/Remove Programs*, then *Windows Components*.
2. Select *Other Network File and Print Services*, then click the *Details* button.

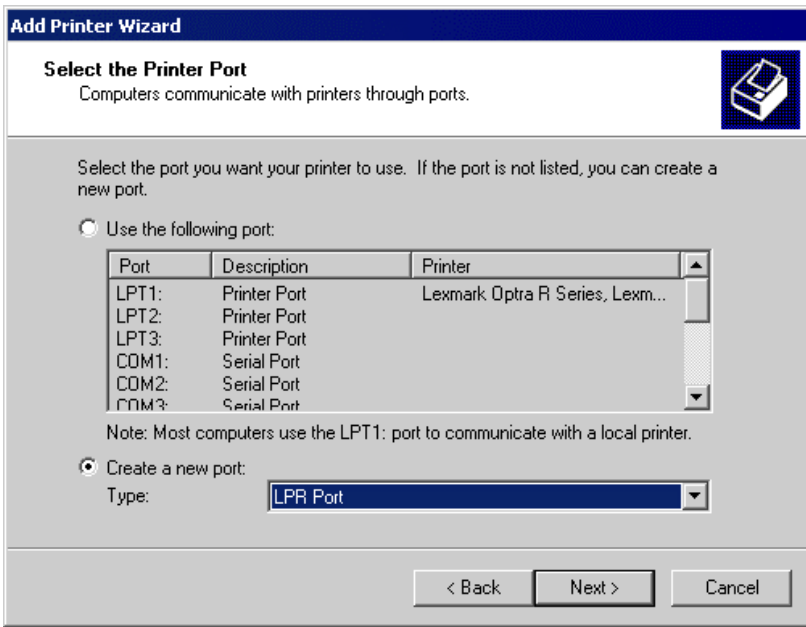


**Figure 16: Adding LPD/LPR Port (Win 2000)**

3. Enable *Print Services for Unix*, and click OK.
4. Click *Next* and complete the Wizard.

## Adding the Printer

1. Open your *Printers* folder, and start the *Add Printer* Wizard.
2. When prompted, select *Local Printer*.
3. On the *Select the Printer Port* screen, select *LPR Port*, as shown below. Click *Next* to continue.



**Figure 17: Windows 2000: Select Port**

4. In the Dialog requesting *Name of Address of server providing lpd*, enter the IP address of the Wireless Gateway.
5. For *Name of printer or print queue on that server*, enter L1.
6. Click OK, and then *Next*, and continue the Wizard.
7. At the *Select Sharing* screen, select the Radio Button for *Share As*, and enter the shared printer name. The shared name is how other users will see this printer. You should advise client PCs of the Server name and this printer name.
8. Complete the *Add Printer* wizard.

## Client PC Setup for LPD/LPR Printing

After configuring the Windows Server, client PCs on the LAN can install the new printer.

The following procedure is for Windows 95/98/ME, Windows NT4.0, and Windows 2000 workstation.

1. Open your *Printers* folder, and start the *Add Printer* Wizard.
2. When prompted, select *Network Printer*.
3. When prompted for *Network Path or Queue Name*, click the *Browse* button, and locate the Server and Printer which your Network Administrator advised you to use.
4. Click OK, then *Next*.
5. Select the correct printer Manufacturer and Model, as advised by your Network Administrator, and click *Next*.
6. Follow the prompts to complete the Wizard.
7. The new printer will be listed with any other installed printers, and may be selected when printing from any Windows application.

## Dial-in Configuration

This section describes how to configure your PC to use the Wireless Gateway's RAS Dial-in feature.

To use the RAS Dial-in feature of the Wireless Gateway:

- An Analog Modem or ISDN TA must be connected to the Serial Port on the Wireless Gateway.
- The Wireless Gateway's *Serial Port* screen must be configured for Dial-in access, and Dial-in Users must be created. See *Chapter 6 - Serial Port* for details.
- A suitable Dial-up connection must be created on your PC, as described below.

### Creating a Dial-in Connection in Windows

You can use the standard Windows *Dial-up Networking* software normally used for Internet access. The procedure is as follows:

1. Ensure your modem is installed and working.
2. Select *My Computer*, then *Dial-up Networking*.
3. Click *Make new Connection*, and step through the Wizard.
  - Give this connection a suitable name.
  - Enter the area code and telephone number to connect to the Wireless Gateway.
  - Continue the Wizard until completed.
4. The default values for this connection will work with the Wireless Gateway's default values. If necessary, you can adjust the *Properties* for the connection:
  - In the *Dial-up Networking* window, select the connection.
  - Right-click, and select *Properties* to see a screen like the one below.

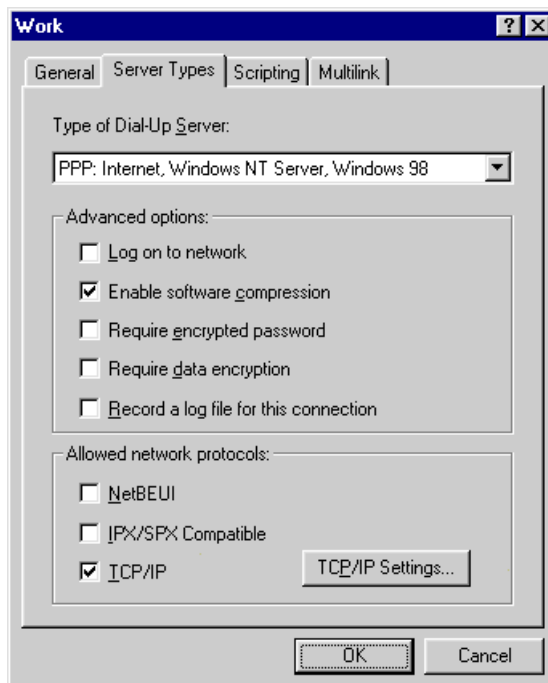


Figure 18: Dial-up Networking Properties

## Dial-up Networking Properties

<b>Log on to network</b>	This setting refers to a logon to a Server on your LAN, not the login to the Wireless Gateway.  This should be disabled; checking this option will cause a minor delay in establishing a connection.
<b>Enable software compression</b>	Normally, this should be checked, but the Wireless Gateway will function with either Checked or Unchecked.
<b>Required encrypted password</b>	The <b>Unchecked</b> state corresponds to the "PAP" setting on the Wireless Gateway's <i>Serial Port</i> screen.  The <b>Checked</b> setting corresponds to the "MSCHAP" setting on the Wireless Gateway's <i>Serial Port</i> screen.
<b>Require data encryption</b>	This must NOT be checked.
<b>Network Protocols</b>	NetBEUI and IPX/SPX can be disabled.
<b>TCP/IP Settings</b>	The default settings should not be changed.

## Using the Dial-in Connection

1. In the *Dial-up Networking* window, double-click the connection to start the dial-in process.
2. When prompted for a user name and password, enter the Name and Password assigned to you (this is done on the Wireless Gateway's *User Details* screen).
3. If the Wireless Gateway's *Callback* feature is enabled, the connection will then be terminated, and your modem must wait for the incoming call from the Wireless Gateway's modem.
4. Upon connection, the Wireless Gateway will allocate an IP Address to your PC. To other LAN users and devices, you will appear to be a normal LAN user.
  - You can connect to any Servers and devices on your LAN which use the TCP/IP network protocol. For example, you can connect to an E-Mail Server, Web Server, or FTP Server on your LAN. If a PC is running NetMeeting, PC Anywhere or similar program, you can connect to that PC.
  - You can use access the Internet through the Wireless Gateway, just like LAN users.
  - You can print to the printer connected to the Wireless Gateway, just as if you were on the LAN.

---

## Macintosh Clients

### Internet Access

From your Macintosh, you can access the Internet via the Wireless Gateway. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

#### Note:

If using manually assigned IP addresses instead of DHCP, the only change required is to set the *Router Address* field to the Wireless Gateway's IP Address.

### Printing

If you wish to share the printer connected to the Wireless Gateway, using a LaserWriter or compatible is strongly recommended.

If the printer connected to the Wireless Gateway is NOT a LaserWriter, ensure that:

- The *Printer Object Type* on the Wireless Gateway's *Printer Port* screen is set correctly.
- Each Macintosh has the correct printer driver for the printer. The Wireless Gateway will not process the print data in any way, but merely forward it to the printer.

### Installing the Printer

To gain access to the printer connected to the Wireless Gateway, follow this procedure:

1. Select *Control Panel - Network*.
2. Ensure that *EtherTalk* is selected under *AppleTalk Connection*.
3. Open *Chooser*, and select the correct printer type (e.g. LaserWriter).
4. From the list of available printers on the right, select the Wireless Gateway, then click *Create*.
5. The new printer will be created, and can be used like any other printer.



## Linux Clients

### Internet Access on Linux

Ensure you are logged in as "root" before attempting any changes.

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the Wireless Gateway.
- Ensure your DNS (Nameserver) settings are correct.

### To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes
  - Use the "Deactivate" and "Activate" buttons, if available.
  - OR, restart your system.

### LPD Printing on Linux

The procedure below may vary according to your version of Linux and X -windows shell.

1. In your X Windows shell, select *Control Panel*, then *Printer Configuration*.
2. Select *Add*. For the printer type, select *Remote Unix (lpd) Queue*.
3. Use the following data to complete the resulting dialog.

Field	Data	Example
<b>Name</b>	Enter a name for this printer	gw_prn
<b>Spool Directory</b>	<i>/var/spool/lpd/printer_name</i> Where <i>printer_name</i> is the "Name" entry above.	<i>/var/spool/lpd/gw_prn</i>
<b>File Limit</b>	Enter a suitable number.	0 (no limit)
<b>Remote Host</b>	Wireless Gateway's IP address  <b>Note:</b> If you have made a host file entry, you can use the name from the host file instead of the IP Address.	192.168.0.1
<b>Remote Queue</b>	<i>Ln</i> Where <i>n</i> is the Logical Printer number (L1, L2, L3). Logical Printers can be configured on the Wireless Gateway's <i>Options- Printer Port</i> screen.	L1

4. Save this data, and exit the Printer Configuration. Configuration is now completed, and the printer is now available for use.

## Other Unix Systems

### For Internet Access via the Wireless Gateway

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless Gateway.
- Ensure your DNS settings are correct.

### LPD Printing

To use LPD printing to the Wireless Gateway's printer, install an LPD printer using the standard procedure for your system.

- Use the Wireless Gateway's IP Address as the location of the remote host
- Use L1, L2, or L3 for the name of the printer on the remote host.

On the Wireless Gateway, the logical printers (L1, L2, and L3) can be configured on the *Options - Printer Port* screen.

## Wireless Station Configuration

This section applies to all Wireless stations wishing to use the Wireless Gateway's Access Point, regardless of the operating system which is used on the client.

To use the Wireless Access Point in the Wireless Gateway, each Wireless Station must have compatible settings, as follows:

<b>Mode</b>	The mode must be set to <i>Infrastructure</i> .
<b>SSID (ESSID)</b>	This must match the value used on the Wireless Gateway. The default value is <b>default</b> <b>Note! The SSID is case sensitive.</b>
<b>WEP</b>	By default, WEP on the Wireless Gateway is <b>disabled</b> . <ul style="list-style-type: none"> <li>• If WEP remains disabled on the Wireless Gateway, all stations must have WEP disabled.</li> <li>• If WEP is enabled on the Wireless Gateway, each station must use the same settings as the Wireless Gateway.</li> </ul>

# Chapter 5

## DHCP

# 5

*This Chapter covers the use of DHCP, using either an existing DHCP Server or the Wireless Gateway's DHCP Server function.*

### Overview

If your LAN does not use DHCP, and you do not wish to use DHCP, you can ignore this chapter.

### What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) **server** allocates a valid IP address to a DHCP **client** (PC or device) upon request.

- The client request is made when the client device boots.
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- Windows 95/98/ME include all the software required to act as a DHCP **client**. This is the default Windows setting for TCP/IP. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".
- The Wireless Gateway can act as a **DHCP server**.

### Using the Wireless Gateway's DHCP Server

This is the default setting. The DHCP Server settings are on the **LAN** screen. On this screen, you can:

- Enable or Disable the Wireless Gateway's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.



**Note!**

**You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.**

### Using another DHCP Server

You can only use one (1) DHCP Server. If you wish to use another DHCP Server, rather than the Wireless Gateway's, the following procedure is required.

1. Disable the DHCP Server feature in the Wireless Gateway. This setting is on the LAN screen.
2. Configure the DHCP Server to provide the Wireless Gateway's IP Address as the *Default Gateway*.

## To Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 95/98/ME. See *Chapter 4 – Client Configuration* for the procedure to check these settings.

# Chapter 6

## Serial Port

# 6

*This Chapter details using the Serial (RS232) Port, either for Internet Access or Dial-in use.*

### Overview

The Serial (RS232) port can be used for Internet Access or to provide RAS (Dial-in) access to your LAN.

- If used for Internet access, the WAN (Ethernet) Port cannot be used.
- Both *Internet Access* and *Dial-in Access* can be enabled simultaneously, but if the modem is in use, a Dial-in user will only get a "busy" signal on their telephone line.

### Serial Port Screen

This screen is reached via the *Serial Port* link on the main menu.

MILAN TECHNOLOGY		ShAir Office™ wireless gateway	
<a href="#">Help</a>			
<b>Modem</b>	Type: <input checked="" type="radio"/> None (Serial Port not used) <input type="radio"/> Permanent connection (leased line) <input type="radio"/> Modem <span>Standard Modem</span>	<a href="#">Modem Properties</a>	
	Serial Line Speed: <span>57600</span> bps		
<b>Internet Access</b>	<input type="checkbox"/> Enable Internet Access <input type="checkbox"/> Dial on Demand <input type="checkbox"/> Disconnect after Idle Time of <span>15</span> min Account/User Name: <input type="text" value="guesst"/> Password: <input type="text"/> Verify: <input type="text"/> IP Address from ISP: <input type="radio"/> Dynamic <input type="radio"/> Fixed <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> DNS IP Address: <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> Telephone: Tel [1] <input type="text" value="0"/> (Required) Tel [2] <input type="text" value="0"/> (Optional) Tel [3] <input type="text" value="0"/> (Optional)		
<b>Dial-in</b>	<input type="checkbox"/> Enable Dial-in <input type="checkbox"/> Disconnect after Idle Time of <span>15</span> min Dial-in PPP Link: <span>PAP</span>		
<b>Dial-in Users</b>	Use this link to create and modify Dial-in Users.		
<b>Status</b>	Use this link to check the status of the Serial Port.		
		<a href="#">Save</a>	<a href="#">Cancel</a>

**Figure 19: Serial Port Screen**

## Data - Serial Port Screen

Modem	
<b>Type</b>	<p>Select <i>None</i> if nothing is connected to the Serial Port, or you do not wish use to use the Serial Port.</p> <p>For <b><i>Permanent Connection (leased line)</i></b>:</p> <ul style="list-style-type: none"> <li>• Ensure the <i>Serial Line Speed</i> is set to match the speed on your leased line.</li> <li>• Ignore the Telephone numbers and "Disconnect after Idle" setting.</li> </ul> <p>For <b><i>Modem</i></b>:</p> <ul style="list-style-type: none"> <li>• If your modem is in the drop-down list, just select it.</li> <li>• If your modem is not in the list, select "_Standard Modem" and test to see if this works.</li> <li>• If "_Standard Modem" does not work, select "Other", then click the <i>Modem Properties</i> button and set these settings correctly. See the section <i>Modem Properties Screen</i> later in this chapter for further details.</li> </ul>
<b>Modem Properties</b>	<p>Clicking this button will open the <b><i>Modem Properties</i></b> screen and allow changing of the modem's properties. Normally, this is not required.</p> <p>See the section <i>Modem Properties Screen</i> later in this chapter for further details.</p>
<b>Serial Line Speed</b>	<p>Select the speed which is equal to or below the fastest <b>Serial</b> line speed (NOT Phone line speed) of your modem. Available speeds range from 4.8K to 460.8K (bps).</p>
Internet Access	
<b>Enable Internet Access</b>	<p>Use this to enable or disable Internet access on this port.</p> <p><b>Checking this box will disable Internet Access via the WAN (Ethernet) port, because both methods cannot be used simultaneously.</b></p> <p>However, for the Serial Port, both Dial-in and Internet can be enabled simultaneously.</p>
<b>Dial on Demand</b>	<p>If checked, an Internet connection will be established automatically, whenever required.</p> <p>If not checked, the Internet connection must be established manually, using the <i>Dial-up</i> button on the <i>Serial Port Status</i> screen.</p>
<b>Disconnect after Idle Time</b>	<p>If checked, an Internet connection will be terminated after the specified time-out period. The allowable range is 1-99 minutes.</p> <p>If not checked, the Internet connection will never be terminated.</p>
<b>Account User Name</b>	<p>Enter the account name provided by your ISP. This name will be used to log in to the ISP's server.</p>
<b>Password</b>	<p>Enter the current password for the above account.</p> <p>Re-enter the password in the <i>Verify</i> field to ensure it is correct.</p>

<b>IP Address from ISP</b>	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> <li>• <b>Dynamic</b> This is the default, and the most common. Leave this selected if your ISP allocates an IP Address to the Wireless Gateway upon connection.</li> <li>• <b>Fixed IP Address</b> Select this if your ISP has allocated you a fixed IP Address, then enter the IP Address in the fields provided.</li> </ul>
<b>DNS IP Address</b>	<p>The DNS (Domain Name Server) translates names (e.g. microsoft.com) to IP Addresses.</p> <p>Enter the DNS IP address supplied or recommended by your ISP.</p> <p>If desired, additional DNS entries can be made on the <i>Options</i> screen.</p>
<b>Telephone</b>	<p>If using a Leased Line (permanent connection), ignore these fields.</p> <p>Otherwise, enter the telephone numbers to dial to connect to your ISP (Internet Service Provider). The first number is required; the others are optional.</p> <p>Enter the telephone numbers using the format described in your modem's user manual.</p>
<b>Dial-In</b>	
<b>Enable Dial-in</b>	<p>If checked, this port is available for dial-in access. Otherwise, any attempt to dial-in will be blocked.</p> <p>If Internet Access is also enabled, Dial-in users may find it difficult to connect because the telephone line is in use. Reducing the <i>Disconnect after Idle Time</i> setting for Internet Access to 1 minute may help.</p> <ul style="list-style-type: none"> <li>• See Dial -in Users later in this Chapter for details of creating and managing dial-in users.</li> <li>• See the <i>Dial-in</i> section in <i>Chapter 4 - PC Configuration</i> for details on setting up the remote PC to use the Wireless Gateway's Dial-in facility.</li> </ul>
<b>Disconnect after Idle Time</b>	<p>If checked, a Dial-in connection will be terminated after the specified time-out period. The allowable range is 1-99 minutes.</p> <p>If preferred, the connection time limit may be set individually for each user.</p>
<b>Dial-in PPP Link</b>	<p>Select the desired security option for log-in:</p> <ul style="list-style-type: none"> <li>• <b>PAP</b> has widespread support; almost all communications systems support it.</li> <li>• <b>CHAP</b> is more secure than PAP; the password is encrypted before transmission. If it is selected, the dial-in clients must also support CHAP in order to connect.</li> <li>• <b>MS CHAP</b> is the Microsoft version of CHAP, used on Windows platforms. If all dial-in clients are using Windows 95 or later, you can choose this option.</li> <li>• <b>None</b> means no login authentication is performed.</li> </ul> <p><b>Warning!</b> If you choose "<b>None</b>", anyone can connect; this is a major security risk.</p>
<b>Links</b>	
<b>Dial-in Users</b>	<p>Use this link to create and manage users for the RAS Dial-in function. See the following section for details.</p>

<b>Status</b>	Use this link to view the <i>Serial Port</i> status screen, described later in this chapter.
---------------	--

## Modem Properties Screen

This screen will be displayed when the "Modem Properties" button on the *Serial Port* screen is clicked. Normally, it is not necessary to access this screen.

Figure 20: Modem Properties Screen

### Data – Modem Properties Screen

Initial String	
<b>Initial String</b>	<p>This is a series of AT commands used to correctly configure your modem or ISDN.</p> <ul style="list-style-type: none"> <li>The <i>Initial String</i> can only be changed for the "Other" modem type.</li> <li>See <b>Appendix C - AT Commands</b> for further details about the required <i>Initial String</i> settings and standard AT commands.</li> </ul>
Other Properties	
<b>Dial Type</b>	Select <i>Tone</i> , <i>Pulse</i> or <i>Other</i> to match your system. For <i>Other</i> , you must provide the <b>Dial String</b> .
<b>Dial String</b>	The AT command sent to your modem before dialing. For example, "ATDT" tells your modem to use Tone Dialing. Check your modem's documentation to find the correct AT commands.
<b>Auto Answer Commands</b>	Enter the command strings which turn the "auto-answer" function in your modem or ISDN TA ON and OFF.



<b>Buttons</b>	
<b>Save</b>	Save the data on this screen.  Note that if the current modem was not "Other" type, and you changed the <i>Initial String</i> , you can NOT use "Save". You must use "Save as Other" instead.
<b>Save as "Other"</b>	Assign the data shown on screen to the "Other" modem type, regardless of the modem selected on the <i>Serial Port</i> screen.  You should then select "Other" as the Modem to use.
<b>Cancel</b>	Reverse any changes since the last "Save" operation.

---

## Dial -in Users

This section describes how to create and manage remote users who wish to use the Wireless Gateway's RAS Dial-in facility.

For details of configuring the remote PC to use Dial-in access, refer to *Dial-in* in *Chapter 4 - Client PC Configuration*.

### Overview

Upon connection, the Wireless Gateway will allocate an IP Address to the Dial-in user. To other LAN users and devices, the Dial-in user will be valid device on the LAN. However, currently Microsoft networking services are not available.

- The Dial-in user can connect to any Servers and devices on your LAN which use the TCP/IP network protocol. For example, the Dial-in user can connect to an E-Mail Server, Web Server, or FTP Server on your LAN. If a PC is running NetMeeting, PC Anywhere or similar program, the Dial-in user can connect to that PC.
- The Dial-in user can use access the Internet through the Wireless Gateway, just like LAN users.
- The Dial-in user can print to the printer connected to the Wireless Gateway, just as if they were on the LAN.

### Controlling Dial-in Access

The Wireless Gateway provides the following options to control Dial-in access:

1. Allow access by anyone and everyone.
  - If Dial-in PPP link security on the Serial Port screen is set to "None", then the user name and password is not checked, so anyone who dials in can gain access.
  - This creates a major security weakness. It is strongly recommended that this option is NOT used.
2. All users use the same log-in.
  - All Dial-in users can use the existing "guest" user, once Dial-in access is Enabled for both the Serial port and the *guest* user.
  - A password should be assigned to the "guest" user. By default, there is no password.
3. Each Dial-in user has a separate log-in and password
  - This is the recommended approach.
  - Each person requiring dial-in access is entered in the Wireless Gateway's user database, using the *Dial-in Users* and *User Details* screens.

## Dial-in Users Screen

This screen is reached via the *Dial-in Users* link on the **Serial Port** screen.

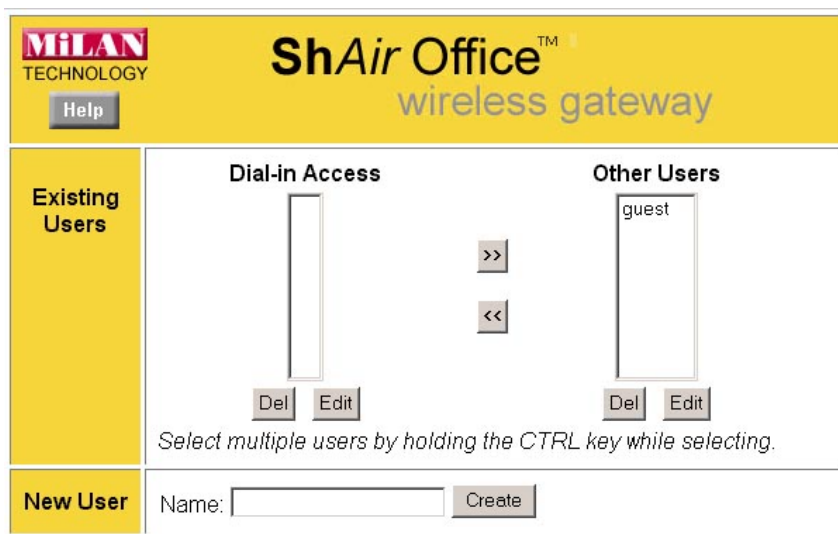


Figure 21: Dial-in Users Screen

## Data – Dial-in Users Screen

Existing Users	
<b>Dial-in Access</b>	<ul style="list-style-type: none"> <li>This lists all users who have Dial-in permission.</li> <li>If no users have dial-in permission, this list will be empty.</li> <li>Select the user or users you wish to change. Multiple users can be selected by holding down the CTRL key while selecting. (For the Macintosh, use the SHIFT key instead of CTRL).</li> </ul>
<b>Other Users</b>	<ul style="list-style-type: none"> <li>This lists all users who do not have Dial-in access.</li> <li>If you have not created any users, this list will contain the pre-defined "guest" user.</li> <li>Use the "Create" button on this screen to create new users as required.</li> <li>Select the user or users you wish to change. Multiple users can be selected by holding down the CTRL key while selecting. (For the Macintosh, use the SHIFT key instead of CTRL).</li> </ul>
New User	
<b>Name</b>	<p>Use this to create new users as required:</p> <ul style="list-style-type: none"> <li>Enter the name for the new user here.</li> <li>Spaces, punctuation, and special characters must NOT be used in the name.</li> <li>User names are case insensitive (case is ignored), so you can not have 2 names which differ only by case.</li> <li>The name can not be changed once the user is created.</li> </ul>

Buttons	
>>	Use the ">>" button to remove Dial-in access for any users selected in the "Dial-in Users" list.
<<	Use the "<<" button to allow Dial-in access for any users selected in the "Other Users" list.
Del	Delete the selected user or users in the list above the button.
Edit	Modify the selected user in the list above the button. Only 1 user should be selected.
Create	This will add a new user to the database. <ul style="list-style-type: none"> <li>Enter the required user name in the "Name" field, then click the <i>Create</i> button.</li> <li>You will then see the "User Details" screen, where you can enter the other details for this user.</li> </ul>

## User Details Screen

This screen is displayed in the following situations:

- Either of the *Edit* buttons on the *Dial-in Users* screen is used to modify the selected user.
- The *Create* button on the *Dial-in Users* screen is used to create a new user.

Figure 22: User Details Screen

## Data – User Details Screen

User ID	
User Name	The user name can not be changed.
Password Verify Password	The password for the current user. Passwords are case sensitive. When creating or changing a password, enter it in the <i>Verify Password</i> field also.

<b>Dial-in</b>	
<b>Enable dial-in access</b>	<p>Use this to suspend or enable dial-in access.</p> <p>This setting can also be changed on the <i>Dial-in Users</i> screen.</p>
<b>Enforce connection time limit</b>	<p>If checked, the Wireless Gateway will terminate the Dial-in connection after the specified period. The time period can be set from 1 to 999 minutes.</p> <p>If unchecked, the connection time-out set on the <i>Serial Port</i> screen will be used. If neither time-out is enabled, the connection must be terminated by the remote user.</p>
<b>Call back</b>	<p>Select the desired option:</p> <ul style="list-style-type: none"><li>• <b>Disabled</b>:- The user can simply dial-in; the Wireless Gateway will not hang-up and call back.</li><li>• <b>Roaming</b>:- After providing their name and password, the user is prompted for the call-back number. The Wireless Gateway will then hang up and dial the number provided by the remote user.</li><li>• <b>Fixed</b>:- The number entered in the <b>Telephone No.</b> field is always used as the call-back number. The Wireless Gateway will accept the incoming call, authenticate the user, then hang up and dial this number.</li><li>• <b>Telephone No</b>:- If <i>Fixed</i> is chosen, a telephone number must be entered in this field. For the other options, this field is ignored.</li></ul>

## Serial Port Status

This screen is reached by either of the following:

- **Status Screen** - *Serial Port Status* link
- **Serial Port Screen** - *Status* link.

An example screen is shown below.

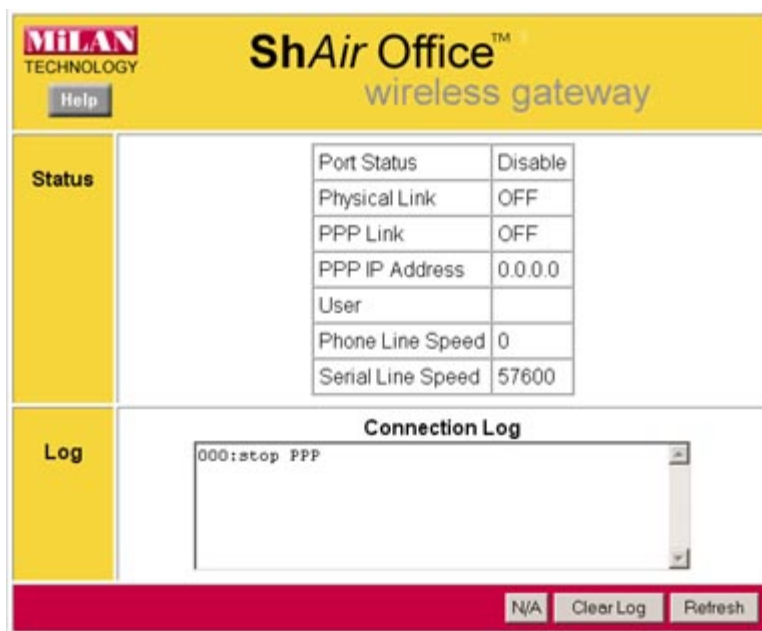


Figure 23: Serial Port Status Screen

### Overview

- **Status** - This section displays the current connection status for the serial port connection.
- **Log** - Displays log messages relating to the connection status.
- **Dial/HangUp Button** - This button will display *Dial* if there is no connection and *Hang-up* if a connection exists. Use this to dial the ISP, or terminate an existing connection. If the Serial Port is Disabled, this button will display "N/A".
- **Clear Log Button** - Clicking this button clears all messages in the log, making new messages easier to read.
- **Refresh Button** - Use this to update the data on screen.

### Data - Serial Port Status Screen

Status	
Port Status	<p>This shows the current port operation. Possible values are:</p> <ul style="list-style-type: none"> <li>• Internet Access</li> <li>• Dial-in</li> <li>• Idle</li> <li>• Disabled</li> </ul> <p>"Disabled" indicates neither Internet Access nor Dial-in is Enabled.</p>

<b>Physical Link</b>	If operating, the link will show ON. This means the modem was able to connect to the number dialed.
<b>PPP Link</b>	If ON, a PPP connection was successfully negotiated.
<b>PPP IP Address</b>	This has 2 possible meanings, depending of the type of connection: <ul style="list-style-type: none"> <li>• <b>Internet Access</b> - This is the IP Address used by this device, as seen by Internet users. This address is provided by your ISP.</li> <li>• <b>Dial-in</b> - This is the IP Address used by the remote user. This IP Address is allocated by the DHCP Server function in the Wireless Gateway.</li> </ul>
<b>User</b>	There are 2 possibilities: <ul style="list-style-type: none"> <li>• For Internet Access, this shows the Internet Account name.</li> <li>• For Dial-in operations, this shows the current user.</li> </ul>
<b>Phone Line Speed</b>	The connection speed over the phone line, between your modem and the number dialed, as reported by your modem.
<b>Serial Line Speed</b>	The connection speed between this device and the modem. This setting can be changed on the <i>Serial Port</i> screen.
<b>Log</b>	
<b>Connection Log</b>	This displays connection details. See below for a description of the most common items in this log.

## Connection Log

This shows the commands sent to the modem, and any status messages returned by the modem. Note that you must click *Refresh* to update the information.

The following table lists the common messages, and their meaning.

Message	Description
Dialing	Dialing the ISP
Try to establish physical connection.	The device is trying to connect with the ISP, using the modem.
Busy	The number dialed was busy.
Physical line is connected	Physical connection to ISP has been established.
CONNECT <i>nnnnnn</i>	Physical connection was successful; <i>nnnnnn</i> indicates the speed of the serial link as currently configured.
Max phone line speed <i>nnnnnn</i> bps	<i>nnnnnn</i> is the maximum speed of the modem, according to the current configuration.
DCD low, DSR low	Physical line break, connection lost.
send "-----" wait "-----"	"AT" commands sent to the modem are displayed as they are sent. Commands in the Script file are also displayed as they are executed.

---

Start PPP	Having established a physical connection, a PPP connection is now being established.
PPP up fail	The PPP connection could not be established.
PPP up successfully	The PPP connection was established successfully.
Stop PPP	The PPP connection was terminated. This will occur at the end of a session, or an error condition.
Try to hang up	Attempting to get the modem to hang up.
Time out	There was no response from the modem
No carrier No answer	The number dialed did not answer.
Idle timer expires	"Disconnect after Idle Time" is Enabled, and the Time-out period has been reached. The connection will now be terminated..
No dial tone	The modem could not obtain a dial tone.
Set baudrate nnnn	The serial line speed is being set to the speed set in the configuration.



# Chapter 7

## Options



This Chapter details the options available on the Wireless Gateway's "Options" screen.

### Overview

An example Options screen is shown below.

MILAN TECHNOLOGY ShAir Office™ wireless gateway	
<b>Password</b>	Setting a password is recommended. New password <input type="text"/> Verify password <input type="text"/>
<b>DNS (Optional)</b>	Secondary DNS IP Address: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> Tertiary DNS IP Address: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<b>NAT</b>	For Internet Access, NAT must remain Enabled. <input checked="" type="checkbox"/> Enable NAT (Network Address Translation)
<b>TFTP</b>	<input type="checkbox"/> Enable Firmware Upgrade using TFTP
<b>Remote Management</b>	<input checked="" type="checkbox"/> Enable Remote Management (administer via the Internet) Port Number: <input type="text" value="8080"/> Current IP Address to connect to this device: 0.0.0.0
<b>Routing table</b>	Only required if your LAN has other Routers.
<b>Printer Port</b>	Settings for Logical Printers and AppleTalk.
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 24: Options Screen

### Password

Once a password is entered, it is required in order to change the device configuration. Passwords are case sensitive and can be up to 8 alphanumeric characters (no spaces or punctuation). To create or change the password, enter the required password in both the *New Password* and *Verify Password* input fields.



**When prompted for the password, leave the "User Name" blank.**

## DNS (Domain Name Server)

- These entries are optional. The main DNS (Domain Name Server) is either provided by your ISP, or entered on the *Quick Setup* screen.
- If desired, enter any other DNS IP Addresses here. The first available DNS will be used.

## NAT (Network Address Translation)

NAT allows PCs on your LAN to share a single external (Internet) IP Address. This IP Address is supplied by your ISP. Use the following to determine whether or not you need NAT.

- For Internet access, NAT **must be left On** unless all PCs on your LAN have valid external IP Addresses.
- If this device is not being used to provide shared Internet access, NAT is not normally required. With NAT disabled, the Wireless Gateway will act as a static router.
- If NAT is disabled, the Firewall protection provided by the Wireless Gateway is lost, and the *Advanced Internet* features (Virtual Servers, Special Applications, and DMZ) are no longer available.

## TFTP

TFTP (Trivial FTP) can be used to upgrade the firmware in the Wireless Gateway. However, this is not normally required; there is a Windows utility available for this purpose.

## Remote Management

This feature allows you to manage the Wireless Gateway via the Internet.

<b>Enable Remote Management</b>	Enable to allow management via the Internet. If Disabled, this device will ignore management connection attempts from the WAN port.
<b>Port Number</b>	Enter a port number between 1024 and 65535 (8080 is recommended). This port number must be specified when you connect (see below).  <b>Note:</b> The default port number for HTTP (Web) connections is port 80, but using port 80 here will prevent the use of a Web "Virtual Server" on your LAN. (See <i>Advanced Internet - Virtual Servers</i> )
<b>Current IP Address</b>	You must use this IP Address to connect (see below).  This IP Address is allocated by your ISP. But if using a Dynamic IP Address, this value can change each time you connect to your ISP. So it is better if your ISP allocates you a Fixed IP Address.

### To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.

- In the "Address" bar, enter "HTTP://" followed by the WAN IP Address of the Wireless Gateway. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)  
e.g.

HTTP://123.123.123.123:8080

This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.

## Routing Table

This link provides access to a standard static routing table.

Configuration is only required if your LAN contains other routers.

Refer to *Chapter 8 - Routing* for further details about Router configuration and using the *Router* screen.

## Printer Port

This link will reveal the **Printer Port** screen, as shown below. Most users do not need to change these settings.



Figure 25: Printer Port Screen

### Data - Printer Port Screen

AppleTalk	
<b>AppleTalk Zone</b>	This determines which Apple systems can gain access to this printer. The default value is *, which allows access by all systems. If you enter another zone name, only Apple systems in that zone will be able to access the printer.

<b>Printer Object Type</b>	<p>Sets the type of printer attached. The default setting is "Laser-Writer". If the attached printer is not a LaserWriter (or compatible), then you must:</p> <ul style="list-style-type: none"> <li>• Install the correct printer driver for the printer on each Apple system requiring printer access</li> <li>• Check your Printer's user manual or manufacturer's Web site and find the correct "Printer Object Type"</li> <li>• Enter the correct "Printer Object Type" on this screen.</li> </ul> <p>If the "Printer Object Type" is incorrect, the printer will not be visible from your Apple system.</p>
<b>Communication Protocol</b>	You must use the same setting as your Macintosh.
<b>Logical Printers</b>	
<b>No (L1, L2, L3)</b>	<p>There are 3 Logical Printers (Ports), named L1, L2, and L3.</p> <p>These names can not be changed, and must be used when selecting the logical printer from your Unix system.</p>
<b>Pre-string (HEX)</b>	Enter (in HEX) the series of printer commands to be sent to the attached printer BEFORE each print job.
<b>Post-string (HEX)</b>	Enter (in HEX) the series of printer commands to be sent to the attached printer AFTER each print job.
<b>LF to CR/LF</b>	If checked, Unix-style LF (line feed) characters at the end of each line will be converted to CR/LF (carriage return/line feed) pairs, as used in MSDOS and Windows.
<b>Printer Status</b>	
<b>Printer Status</b>	<p>This indicates the current status of the printer. Possible values are:</p> <ul style="list-style-type: none"> <li>• Idle</li> <li>• Printing</li> <li>• Off-line</li> <li>• Out of paper</li> </ul>
<b>"Refresh" Button</b>	Click this to update the printer status information

# Chapter 8

## Routing



*This Chapter explains the Routing features of the Wireless Gateway.*

### Overview

- If you don't have other Routers or Gateways on your LAN, ignore the "Routing" page completely.
- If the Wireless Gateway is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.
- If your LAN has a standard Router (e.g. Cisco) on your LAN, and the Wireless Gateway is to act as a Gateway for all LAN segments, enable RIP (Routing Information Protocol) and ignore the Static Routing table.
- If your LAN has other Gateways and Routers, and you wish to control which LAN segments use each Gateway, do NOT enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers.)
- If using Windows 2000 Datacenter Server as a software Router, enable RIP on the Wireless Gateway, and ensure the following Windows 2000 settings are correct:
  - Open *Routing and Remote Access*
  - In the console tree, select *Routing and Remote Access*, [server name], *IP Routing*, *RIP*
  - In the "Details" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".
  - On the "General" tab, set *Outgoing packet protocol* to "RIP version 2 broadcast", and *Incoming packet protocol* to "RIP version 1 and 2".

### Routing Screen

The routing table is accessed by the *Routing* link on the *Options* screen.

### Using this Screen

Generally, you will use either RIP (Routing Information Protocol) OR the Static Routing Table, although it is possible to use both methods simultaneously.

#### Static Routing Table

If RIP is not used, an entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached.

The other Routers must also be configured. See Router Configuration later in this chapter for further details and an example.

Figure 26: Routing Screen

## Data - Routing Screen

RIP	
<b>Enable RIP</b>	<p>Check this to enable the RIP (Routing Information Protocol) feature of the Wireless Gateway.</p> <p>The Wireless Gateway supports RIP 1 only.</p>
Static Routing Table	
<b>Select Entry</b>	<p>This drop-down list shows all entries in the Routing Table.</p> <ul style="list-style-type: none"> <li>To view or change an entry, select it, then click the <i>Get Data</i> button.</li> <li>After making any required changes, click the <i>Update</i> button to save your changes.</li> </ul>
<b>Destination IP Address</b>	<p>The network address of the remote LAN segment.</p> <p>For standard class "C" LANs, the network address is the first 3 fields of this <i>Destination IP Address</i>. The 4<sup>th</sup> (last) field can be left at 0.</p>
<b>Network Mask</b>	<p>The Network Mask used on the remote LAN segment. For class "C" networks, the standard Network Mask is 255.255.255.0</p>
<b>Gateway IP Address</b>	<p>The IP Address of the Gateway on the LAN segment to which this device is attached. (NOT the router on the remote LAN segment.)</p>
<b>Interface</b>	<p>Select the appropriate interface - LAN (Internal LAN) or WAN (External LAN or WAN) from the drop-down list.</p>
<b>Metric</b>	<p>The number of routers which must be traversed to reach the remote LAN segment. The default value is 1.</p>
Buttons	
<b>Clear Form</b>	<p>Clears all data, ready for input of a new entry.</p>
<b>Add</b>	<p>Add a new entry to the Routing table, using the data shown on screen.</p> <p>The name shown in the drop-down list is ignored.</p>

<b>Delete</b>	Delete the entry selected in the drop-down list, regardless of whether its details are shown on screen.
<b>Update</b>	Update the entry selected in the drop-down list, using the data shown on screen.
<b>List All</b>	List all entries in the Routing table.
<b>Save</b>	Save the RIP setting. This has no effect on the Static Routing Table.
<b>Cancel</b>	Reverse any changes made since the last "submit" operation (i.e. since clicking any other button).

## Router Configuration

It is essential that all IP packets for devices not on the local LAN be passed to the Wireless Gateway, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the Wireless Gateway as the *Default Route* or *Default Gateway*.

### Local Router

The local router is the Router installed on the same LAN segment as the Wireless Gateway. This router requires that the *Default Route* is the Wireless Gateway itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

<b>Destination IP Address</b>	Normally 0.0.0.0, but check your router documentation.
<b>Network Mask</b>	Normally 0.0.0.0, but check your router documentation.
<b>Gateway IP Address</b>	The IP Address of the Wireless Gateway.
<b>Metric</b>	1

### Other Routers on the Local LAN

Other routers on the local LAN must use the Wireless Gateway's *Local Router* as the *Default Route*. The entries will be the same as the Wireless Gateway's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the Wireless Gateway's local Router, the *Gateway IP Address* is the address of the Wireless Gateway's local router.
- For routers which must forward packets to another router before reaching the Wireless Gateway's local router, the *Gateway IP Address* is the address of the intermediate router.

## Static Routing - Example

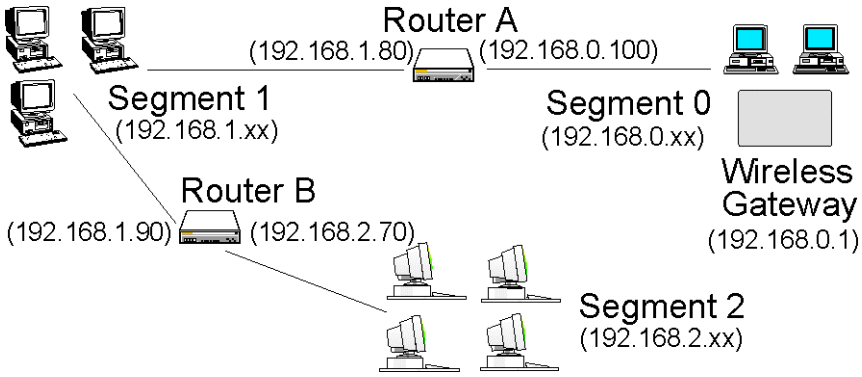


Figure 27: Routing Example

### For the Wireless Gateway's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the Wireless Gateway requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (Wireless Gateway's local Router)
Interface	LAN
Metric	1
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Interface	LAN
Metric	2

### For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (Wireless Gateway's IP Address)

### For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (Wireless Gateway's local router)



# Advanced Internet

*This Chapter explains how to use the Wireless Gateway's "Advanced Internet" features.*

## Overview

For situations where the Wireless Gateway is being used to provide shared Internet access, the following advanced features are provided.

- Special Internet Applications
- URL Filter
- Virtual Servers
- DMZ

This chapter contains details of the configuration and use of each of these features.

## Advanced Internet Screen

This screen provides access to the advanced Internet features, and provides a convenient overview and control center. An example screen is shown below.

MILAN TECHNOLOGY		ShAir Office™ wireless gateway	
<a href="#">Help</a>			
<b>Special Internet Applications</b>	Configure this device to allow use of non-standard Internet applications, such as Video-conferencing, 2-way communication, and Games Servers.		
<b>URL Filter</b>	Block access to specified Web Site.		
<b>Virtual Servers</b>	Allow Internet users to access Servers on your LAN. Without this feature, access would be blocked by the Firewall in this device.		
<b>User-Defined Virtual Servers</b>	Define non-standard Virtual Servers using port numbers.		
<b>DMZ</b>	Allows unrestricted 2-way Internet communication by 1 computer.		
<b>Operation</b>	Special Internet Applications	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
	URL Filter	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
	Virtual Servers	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
	DMZ	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
		<a href="#">Save</a>	<a href="#">Cancel</a>

**Figure 28: Advanced Internet Screen**

On this screen, you can enable or disable any required feature.

## Special Internet Applications

This feature is only required if you wish to use Internet applications which require 2-way communication, multiple connections, or combined TCP/UDP connections.

Examples of such applications are Internet Videoconferencing, Telephony, Games Servers, and other special-purpose Servers.

Generally, you will become aware of the need for this feature when an Internet application is unable to function correctly.



**Note!**

**At any time, only one (1) PC can use each Special Application.**

## Special Applications Screen

This screen can be reached by selecting *Special Internet Applications*. An example screen is shown below.

Details	Name	Protocol	Port Range: Start	Port Range: Finish
Outgoing	dialpad	UDP	51200	51201
Incoming	dialpad	UDP	51200	51201

**Figure 29: Special Applications Screen**

## Using a Special Application

- Ensure that *Special Applications* has been enabled on the *Advanced Internet* screen.
- Configure the *Special Applications* screen as required.



**Note!**

**Configuration data must be obtained from the Service/Application provider.**

**If an application still cannot function correctly, try using the "DMZ" feature.**

Some Special Applications have been defined but not enabled.

## Managing Special Application Entries

- Enable**
1. Select the entry from the drop-down list
  2. Click "Get Data"
  3. Check the *Enable* checkbox
  4. Click "Update"
- Disable** As above, but uncheck the *Enable* checkbox.
- Disable all** On the *Advanced Internet* screen, you can Enable or Disable the *Special Applications* feature.
- Delete**
1. Select the entry from the drop-down list
  2. Click "Delete"
- Modify (Edit)**
1. Select the entry from the drop-down list
  2. Click "Get Data"
  3. Make any desired changes
  4. Click "Update"
- Create a new entry**
1. Click "Clear Form"
  2. Enter the required data, as described below.
  3. Click "Add".

## Data - Special Applications Screen

This data must be obtained from the service provider.

Select Entry	
<b>Name</b>	This drop-down list shows all <i>Special Applications</i> which have been defined.
<b>Get Data Button</b>	After selecting the desired entry, click this button to view its current settings in the <i>Details</i> section of the screen.  You can then make any changes required. Click the "Update" button to save your changes.
Details	
<b>Name</b>	Enter a descriptive name to identify this application entry.
<b>Enable</b>	Use this to Enable or Disable support for this application, as required.
Outgoing	
Protocol	The protocol (TCP or UDP) used when you connect to the special application service.
Port Range: Start	The beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.
Port Range: Finish	The end of the range of port numbers used by the application server, for data you send.

<b>Incoming</b>	
Protocol	The protocol (TCP or UDP) used when the application or service sends data to you.
Port Range: Start	The start of the range of port numbers used by the application server when data is sent to you. If using only one port number, enter it in both the "Start" and "Finish" fields.
Port Range: Finish	The end of the range of port numbers used by the application server, when data is sent to you.
<b>Buttons</b>	
<b>Clear Form</b>	Clears all data, ready for input of a new entry.
<b>Add</b>	Add a new entry to the Special Applications database, using the data shown on screen. The name shown in the drop-down list is ignored.
<b>Delete</b>	Delete the Special Application entry selected in the drop-down list, regardless of whether its details are shown on screen.
<b>Update</b>	Update the Special Application entry selected in the drop-down list, using the data shown on screen.
<b>List All</b>	List all Special Application entries.
<b>Cancel</b>	Reverse any changes made since the last "submit" operation (i.e. since clicking any other button).

## URL Filter

The *URL Filter* provides a means to block access to undesirable Web sites. The blocking action applies to all PCs accessing the Internet via the Wireless Gateway.

### Operation

The *URL Filter* feature works by matching the "Filter Strings" (text strings) against the requested URL. For example, by inputting the word "bad" in the *URL Filter*, any URL containing the letters "bad" in it will be blocked.

Note that if **any component** of the URL request contains one of the "Filter Strings", that request will be blocked while the *URL Filter* is enabled.

URL requests to Web (Internet) Servers include the following components:

- **Protocol.** For Internet access, the usual protocol is HTTP (shown in your browser as "HTTP://"). The URL Filter works **ONLY** with the HTTP protocol. Other protocols, such as FTP and E-Mail, are not affected by the URL Filter.
- **Domain.** This is the address of the site (e.g. www.microsoft.com)
- **Path.** This specifies a certain file on the Server (e.g. /public/docs/index.html )
- **Parameters.** This is the data which is sent (submitted) to the Server when you submit a form, such as when you use a search engine to search the Internet.  
On a Web page, clicking a link may also submit data to a Server, rather than just request a file.

**All of these components are searched to see if they contain any of the "Filter Strings".**

### Tips

- To use the *URL Filter* feature properly, you should try inputting as much of the text for the given URL as possible. For example, instead of simply using the word "bad," you could use the full web site name.
- If you do not want to block an entire web site, you can include the path rather than just the domain. For example, "www.badsite.com/badsection/"
- Be careful when using the *URL Filter*, as a general word might block access to many other sites as well as the one that you intend to block.
- You can use the *Internet Access Log*, accessed from the **Status** screen, to see which sites have been blocked by the *URL Filter*.

## URL Filter Screen



Figure 30: URL Filter Screen

### Data - URL Filter Screen

Site List	
<b>Site List</b>	This lists any existing entries. If you have not entered any values, this list will be empty.
<b>Filter String</b>	To add an entry to the list, enter it here, and click the "Add" button. An entry may be a Domain name (e.g. www.trash.com) or simply a string (e.g. ads/ ) Any URL which contains ANY entry ANYWHERE in the URL will be blocked.
<b>Buttons</b>	<b>Delete/Delete All</b> - Use this buttons to delete the selected entry or all entries, as required. Multiple entries can be selected by holding down the CTRL key while selecting. (On the Macintosh, hold the SHIFT key while selecting.) <b>Add</b> - Use this to add the current <i>Filter String</i> to the site list.



You can use the *Internet Access Log*, accessed from the *Status* screen, to see which sites have been blocked by the URL Filter.

## Virtual Servers

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

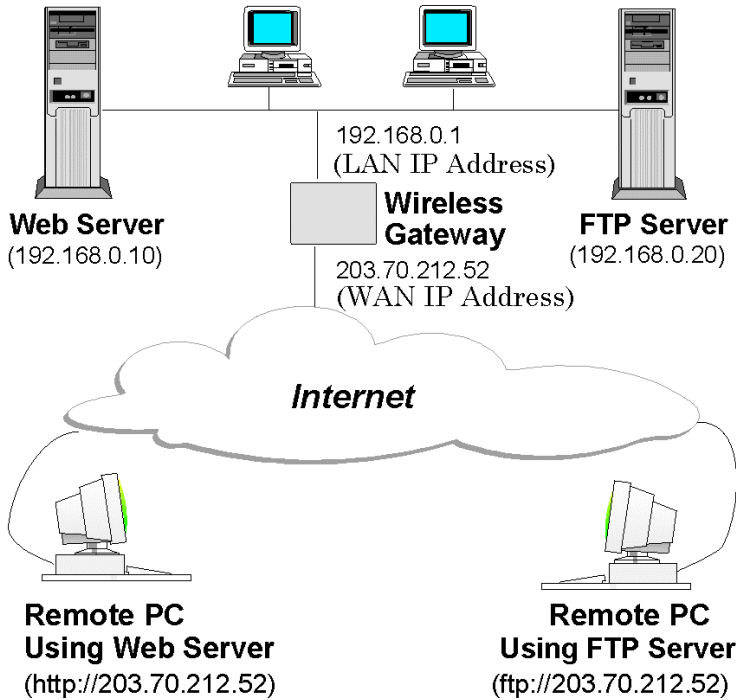


Figure 31: Virtual Servers

## IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

**To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.**

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. If using a Static IP Address, it is entered on the "WAN" screen.

## Types of Virtual Servers

The Wireless Gateway supports two (2) types of Virtual Servers:

- **Pre-defined** - Standard server types. The only data required is the IP Address of the server on your LAN.
- **User-defined** - Non-standard servers. You must provide additional information about the server.

**Note:** The TOTAL number of Virtual Servers which can be used at any time is 10.

## Virtual Server Screen

The *Virtual Servers* screen is reached by the *Advanced Internet - Virtual Servers* link.

WAN IP Address		
Current IP Address to connect to ALL Virtual Servers: This address is allocated by your ISP. It is better to have a fixed IP Address.		
Virtual Servers		
Type of Server	Enable	LAN IP Address
DNS	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Finger	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
FTP	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Gopher	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Mail (SMTP)	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Mail (POP3)	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
News	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Telnet	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Web	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Whois	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Figure 32: Virtual Server Screen.

### Data – Virtual Server Screen

WAN IP Address	
<b>Current IP Address</b>	This shows the IP Address which Internet users must use to connect to any of your Virtual Servers. <ul style="list-style-type: none"> <li>To Internet Users, ALL of your Virtual Servers have the same IP Address.</li> <li>This IP Address is allocated by your ISP. It is better to have a fixed IP Address.</li> </ul>
Virtual Servers	
<b>Type</b>	Select the type of Server you wish to use.
<b>Enable</b>	Check to enable this Server.



<b>LAN IP Address</b>	<ul style="list-style-type: none"> <li>• Enter the IP Address of a PC on your LAN.</li> <li>• You must install and configure the appropriate Server software on the PC entered here.</li> <li>• If using DHCP, the LAN IP Address of a PC may change. To solve this problem, use either of these methods: <ul style="list-style-type: none"> <li>• Assign a fixed IP Address to the Server PC, ensuring that its IP Address is NOT within the address range allocated by the DHCP Server.</li> <li>• Reserve an IP Address for the Server PC in the DHCP Server, using the <i>Access Control - PC</i> screen.</li> </ul> </li> </ul>
-----------------------	--

**Note!**

**For each entry, the PC must be running the appropriate Server software.**

## User Defined Virtual Servers

If the type of Server you wish to use is not listed on the *Virtual Servers* screen, you can define it using this feature.

Select *Advanced Internet - User Defined Virtual Servers* to see a screen like the example below.

The screenshot shows the 'User Defined Virtual Servers' configuration page. At the top, there is a yellow header with the 'MILAN TECHNOLOGY' logo on the left and 'ShAir Office™ wireless gateway' on the right. Below the header is a 'Help' button. The main content area is divided into three sections:

- WAN IP Address:** Shows the current IP address as 0.0.0.0 and a note that this is allocated by the ISP.
- Select Server:** Includes a 'Name' dropdown menu, a 'Get Data' button, and a note to click 'Get Data' for correct data.
- Details:** Contains input fields for 'Name', 'IP Address' (with four individual boxes for each digit), 'Protocol' (set to UDP), 'Internal Port No.' (required), and 'External Port No.' (optional). There is also an 'Enable' checkbox and a 'Clear Form' button.

At the bottom of the page, there is a red bar with buttons for 'Add', 'Delete', 'Update', 'List All', and 'Cancel'.

**Figure 33: User Defined Virtual Servers**

## Managing User Defined Virtual Servers

- Enable a Server**
1. Select the required entry from the drop-down list
  2. Click "Get Data"
  3. Check the *Enable* checkbox
  4. Click "Update"
- Disable a Server** As above, but uncheck the *Enable* checkbox.
- Disable all Servers** On the *Advanced Internet* screen, you can Enable or Disable the *Virtual Servers* feature.
- Delete**
1. Select the entry from the drop-down list
  2. Click "Delete"
- Modify (Edit)**
1. Select the entry from the drop-down list
  2. Click "Get Data"
  3. Make any desired changes
  4. Click "Update"
- Create a new entry**
1. Click "Clear Form"
  2. Enter the required data, as described below.
  3. Click "Add".

## Data- User Defined Virtual Servers Screen

WAN IP Address	
<b>Current IP Address</b>	<p>This shows the IP Address which Internet users must use to connect to any of your Virtual Servers.</p> <ul style="list-style-type: none"> <li>• To Internet Users, ALL your Virtual Servers have the same IP Address.</li> <li>• This IP Address is allocated by your ISP. It is better to have a fixed IP Address.</li> </ul>
Select Server	
<b>Name</b>	This lists any Servers you have defined. Click the "Get Data" button to view the correct data for the selected Server.
<b>Get Data Button</b>	<p>After selecting the desired entry, click this button to view its current settings in the <i>Details</i> section of the screen.</p> <p>You can then make any changes required. Click the "Update" button to save your changes.</p>
Details	
<b>Name</b>	Enter a descriptive name to identify this Server entry.
<b>Enable</b>	Use this to Enable or Disable support for this Server, as required.
<b>IP Address</b>	The IP Address of the PC on your LAN which is running the Server software.
<b>Protocol</b>	Select the protocol (TCP or UDP) used by the Server.

<b>Internal Port Number</b>	Enter the port number used by the Server to connect to clients.
<b>External Port Number</b>	The port number used by clients when connecting to the Server. This is normally the same as the <i>Internal Port Number</i> . If it is different, this device will perform a "mapping" or "translation" function, allowing the server to use one port address, while clients use a different port address.
<b>Buttons</b>	
<b>Clear Form</b>	Clears all data, ready for input of a new entry.
<b>Add</b>	Add a new entry, using the data shown on screen. The name shown in the drop-down list is ignored.
<b>Delete</b>	Delete the Virtual Server entry selected in the drop-down list, regardless of whether its details are shown on screen.
<b>Update</b>	Update the Virtual Server entry selected in the drop-down list, using the data shown on screen.
<b>List All</b>	List all User-defined Virtual Servers.
<b>Cancel</b>	Reverse any changes made since the last "submit" operation (i.e. since clicking any other button).

**Note!**

**From the Internet, ALL Virtual Servers have the IP Address allocated by your ISP, as shown by the "WAN IP Address".**

## Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the WAN Port IP Address (the IP Address allocated to this device by your ISP).

e.g.

`http://203.70.212.52`

`ftp://203.70.212.52`

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. If using a Fixed IP Address, it is entered on the *WAN* screen.

## DMZ

This feature, if enabled, allows one (1) computer on your LAN to be exposed to all users on the Internet, allowing unrestricted 2-way communication between the "DMZ" PC and other Internet users or Servers.

This allows connection to special-purpose servers which require proprietary client software, or 2-way user connections such as Video-conferencing, which requires both users to run special software.



**Note!**

**To allow unrestricted access, the Firewall in this device is disabled, creating a security risk.**

**You should use this feature only if the "Special Applications" feature is insufficient to allow an application to function correctly. This feature should be turned ON only when needed, and left OFF the rest of the time.**

## DMZ Screen

Select *Advanced Internet* from the navigation bar, then *DMZ*. You will see a screen like the following:

**Figure 34: DMZ Screen**

### Data – DMZ Screen

Enable	
<b>Enable DMZ Feature</b>	Use this to Enable or Disable the DMZ feature. The DMZ feature should be disabled when not required.
LAN IP Address	
<b>LAN IP Address</b>	Enter the IP Address of the PC on your LAN which will become the "DMZ" PC.

	<p>If using DHCP, the LAN IP Address of a PC may change. To solve this problem, you can use either of these methods:</p> <ul style="list-style-type: none"><li>• Assign a fixed IP Address to the DMZ PC, ensuring that its IP Address is NOT within the address range allocated by the DHCP Server.</li><li>• Reserve an IP Address for the DMZ PC in the DHCP Server, using the <i>Access Control - PC</i> screen.</li></ul>
<b>WAN IP Address</b>	
<b>WAN IP Address</b>	<p>This is the IP Address that Internet users must use to connect to the "DMZ" PC.</p> <p>This IP Address is allocated by your ISP. It is better if you are using a fixed IP Address, so that it never changes. This will make it easier for Internet users to connect to you. If using a Static IP Address, it is entered on the "WAN" screen.</p>



**To Internet users, the IP Address of the DMZ computer is the IP Address allocated by your ISP, as shown by the "WAN IP Address".**

# Access Control

*This Chapter explains how to configure and use the Wireless Gateway's "Access Control" feature.*

## Overview

The Access Control feature allows administrators to restrict Internet Access by individual PCs. The process uses "Packet Filtering" to block or discard data packets. By default, no packets are blocked or discarded.

### To use this feature:

- Set the desired restrictions on the "Everyone" group. All PCs are in the "Everyone" group unless explicitly moved to another group, using the *PC* screen.
- Set the desired restrictions on the other groups ("Group 1", "Group 2", etc) as needed.
- For each PC you wish to move from the "Everyone" group, enter their details on the *PCs* screen, and assign them to the desired group.



**Note!**

**You can limit Internet access for ALL PCs without entering ANY PC data. Simply apply the desired restrictions to the "Everyone" group.**

It is also possible to define your own packet filters, and use these filters in addition to the pre-defined filters. Defining your own filters is optional.

## Access Control Log

This log is accessed from the *Access Control Log* on the **Status** screen. It shows the attempted accesses which have been blocked.

This log can be used to track the operation of the *Access Control* feature. Data shown in this log is as follows:

- **Port** - The port used to gain access to this device. Possible values are LAN, WAN, WLAN (Wireless LAN), and RS232 (serial port).
- **Source IP Address** - The IP Address of the PC or device whose access request was blocked.
- **Physical Address (Hardware Address)** - The hardware address of the PC or device whose access request was blocked.
- **Name** - If known, the name of the device whose access was blocked. This name is taken from the *Access Control* database. For Wireless devices, the name is obtained from the *Wireless Stations* list, and so will always match the Physical (Hardware) address.
- **Destination** - The destination of the attempted access. Possible values are "Internet", "LAN" or "WLAN".
  - "Internet" indicates an outgoing connection attempt which was blocked by the *Access Control* feature.
  - "LAN" or "WLAN" represents an inward connection attempt which was blocked by the Firewall. These inward connection attempts are not affected by the *Access Control* settings.

## Security Groups Screen

The *Security Groups* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.

**MILAN TECHNOLOGY** **ShAir Office™** wireless gateway

Help

**Security Group** Select Group:    
Click "Get Data" to see correct data for selected group.

**Access Rights** Internet Access for this Group:  
 No restrictions  
 Block all Access  
 Use Packet Filter Table below

**Packet Filter Table** Check the items you wish to block (discard).

Applications to Block	TCP Packets to Discard
<input type="checkbox"/> Archie	6667 Chat
<input type="checkbox"/> DNS	79 Finger
<input type="checkbox"/> E-Mail	7070 Raudio
<input type="checkbox"/> FTP	Select items to block.
<input type="checkbox"/> Gopher	Created on "Filters" screen
<input type="checkbox"/> News	<b>UDP Packets to Discard</b>
<input type="checkbox"/> SNMP	Select items to block.
<input type="checkbox"/> Telnet	Created on "Filters" screen
<input type="checkbox"/> TFTP	
<input type="checkbox"/> WWW	

**Figure 35: Security Groups Screen**

Note that the Security groups are pre-named "Everyone", "Group 1", "Group 2", "Group 3", and "Group 4".

## Operations

### Define Access Rights for a Security Group

1. Select the group from the drop-down box.
2. Enter the required data as described below.  
If necessary, click *Clear Form* to remove the existing information shown on screen.
3. Click the *Save* button when finished.

### Change Access Rights for a Security Group

1. Select the group from the drop-down box,
2. Click *Get Data* to view their information
3. Change any fields you wish.
4. Click *Save* when finished.

### Assign PCs to a Security Group

All PCs are initially in the "Everyone" group. Use the *PCs* screen to move individual PCs to other groups as required.

## Data – Security Groups Screen

The following data is required.

<b>Access Rights: Internet Access for this Group</b>	
<b>No restrictions</b>	No packets are blocked. Use this to create an "Unlimited Access" group, or to temporarily remove restrictions.
<b>Block all Access</b>	Groups members cannot access the Internet at all. Use this to create the most restrictive group.
<b>Use Packet Filter Table below</b>	Use this to define intermediate levels of access. Using the Packet Filter table gives you fine control over Internet access.  Simply select the items you wish to block. You can choose from the pre-defined filters in the <i>Applications to Block</i> column, or your own filters in the <i>TCP Packets to Discard</i> and <i>UPD Packets to Discard</i> column.

<b>Packet Filter Table</b>	
<b>Applications to Block</b>	Any items checked will be blocked. Users will not be able to use the application.
<b>TCP Packets to Discard</b>	This lists any TCP filters you have defined on the <i>Filters</i> screen. If no filters have been defined, this is empty. Multiple items can be selected (or deselected) by holding down the Ctrl key while selecting items. Selected items can NOT be accessed by members of this group.
<b>UDP Packets to Discard</b>	This lists any UDP filters you have defined on the <i>Filters</i> screen. If no filters have been defined, this is empty. Multiple items can be selected (or deselected) by holding down the Ctrl key while selecting items. Selected items can NOT be accessed by members of this group.



**Note!**

**If you have not defined your own filters, but wish to do so, refer to "Filters" later in this chapter.**



## PCs Screen

The *PCs* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.

**Figure 36: PCs Screen**

Note that the drop-down box lists all PCs previously entered. If none have been entered, this box will be empty.

## Operations

### Create a new entry

1. Click the "Clear Form" button.
2. Enter the required data, as described below.
3. Click "Add".

Note: The name shown in the drop-down list is ignored.

### Delete an entry

1. Select the entry from the drop-down list
2. Click "Delete"

### Modify (Edit) an entry

1. Select the entry from the drop-down list.
2. Click "Get Data" to view the current data for this entry.
3. Make any desired changes
4. Click "Update"

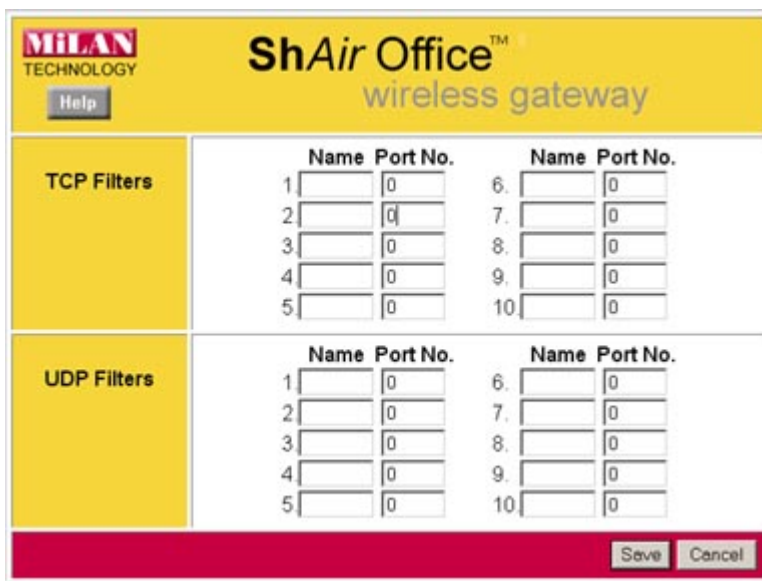
## Data – PCs Screen

Select PC	
PC Name	This drop-down list shows all entries in the "PC" database. If you have not made any entries, this list will be empty.
Get Data button	Click this button to view the data for the PC selected in the drop-down list. You can then edit the data.

<b>Details</b>	
<b>PC Name</b>	Enter a name to identify this PC.
<b>Network Adapter Address</b>	Hardware address for this PC. You can use the Windows "Winipcfg" program or your LAN management program to find this address.
<b>Reserve entry in DHCP Table</b>	<p>Check this if you wish to reserve an IP address for this PC. This is useful if you have to provide the IP Address for other programs or users.</p> <p>If this is left unchecked, the following entry can be ignored.</p>
<b>Reserved IP Address</b>	This relates to the entry above. Enter the reserved address here. This <b>MUST</b> be within the range used by the DHCP server (set on the <i>Device - Internal LAN Port</i> screen).
<b>Security Group</b>	Select the security group for this PC. If you only wish to reserve an IP Address, and are not using the security (access control) features, simply leave this at "Everyone".
<b>Buttons</b>	
<b>Clear Form</b>	Clears all data, ready for input of a new entry.
<b>Add</b>	<p>Add a new entry, using the data shown on screen.</p> <p>The name shown in the drop-down list is ignored.</p>
<b>Delete</b>	Delete the Virtual Server entry selected in the drop-down list, regardless of whether its details are shown on screen.
<b>Update</b>	Update the Virtual Server entry selected in the drop-down list, using the data shown on screen.
<b>List All</b>	List all User-defined Virtual Servers.
<b>Cancel</b>	Reverse any changes made since the last "submit" operation (i.e. since clicking any other button).

## Filters Screen

The *Filters* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.



**Figure 37: Filters Screen**

This screen allows you to define packet filters. When you define security groups, on the "Security Groups" screen, you can select from any filters defined here, as well as the pre-defined filters.

## Data – Filters Screen

Define the packets you wish to be filtered out, by entering the following data.

TCP Filters	
<b>Name</b>	Enter a descriptive name for this entry.
<b>Port No.</b>	Enter an integer representing the Port Number for this type of packet. This information can normally be provided by the service provider. Otherwise, a Network Analyzer or Packet Sniffer can be used to determine the correct port number.
UDP Filters	
<b>Name</b>	Enter a descriptive name for this entry.
<b>Port No.</b>	Enter an integer representing the Port Number for this type of packet. This information can normally be provided by the service provider. Otherwise, a Network Analyzer or Packet Sniffer can be used to determine the correct port number.

# Appendix A

## Troubleshooting



*This Appendix covers the most likely problems and their solutions.*

### Overview

This chapter covers some common problems that may be encountered while using the Wireless Gateway and some possible solutions to them. If you follow the suggested steps and the Wireless Gateway still does not function properly, contact your dealer for further advice.

### General Problems

**Problem 1:** Can't connect to the Wireless Gateway to configure it.

**Solution 1:** Check the following:

- The Wireless Gateway is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Wireless Gateway are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure that your PC is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the Wireless Gateway's default IP Address of 192.168.0.1.

Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Gateway.

In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

### Internet Access

**Problem 1:** When I enter a URL or IP address I get a time out error.

**Solution 1:** A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct (IP address, Network Mask, Default gateway and DNS).
- If the PCs are configured correctly, but still not working, check the Wireless Gateway. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If the Wireless Gateway is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

**Problem 2:** Some applications do not run properly when using the Wireless Gateway.

**Solution 2:** The Wireless Gateway processes the data passing through it, so it is not transparent.

Use the *Special Applications* feature to allow the use of Internet applications

which do not function correctly.

If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.
- When the *DMZ* feature is being used, the *Special Applications* and *Virtual Server* features should be disabled.

## Wireless Access

**Problem 1:** My PC can't locate the Wireless Access Point.

**Solution 1:** Check the following.

- Your PC is set to *Infrastructure Mode*.
- The wireless channel used matches the wireless channel on the Access Point.
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless Access Point must have the same setting for WEP. The default setting for the Wireless Gateway is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled, the key tables must match.
- If the Wireless Station access permission on the Wireless Gateway's *Wireless* screen is set to *Only allow access if on this list*, then each Wireless station must have its address correctly entered.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point. Remember that the connection range can be as little as 100 feet in poor environments.

**Problem 2:** Wireless connection speed is very slow.

**Solution 2:** The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

- Access Point location.  
Try adjusting the location and orientation of the Access Point.
- Wireless Channel  
If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference  
Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding  
Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Access Point.

## Printing

**Problem 1:** When I tried to install the Printing software for Peer-to-Peer printing, I received an error message and the installation was aborted.

**Solution 1:** This may be caused by an existing installation of the printer port software. Before attempting another installation:

- Remove the existing installation
- Restart your PC

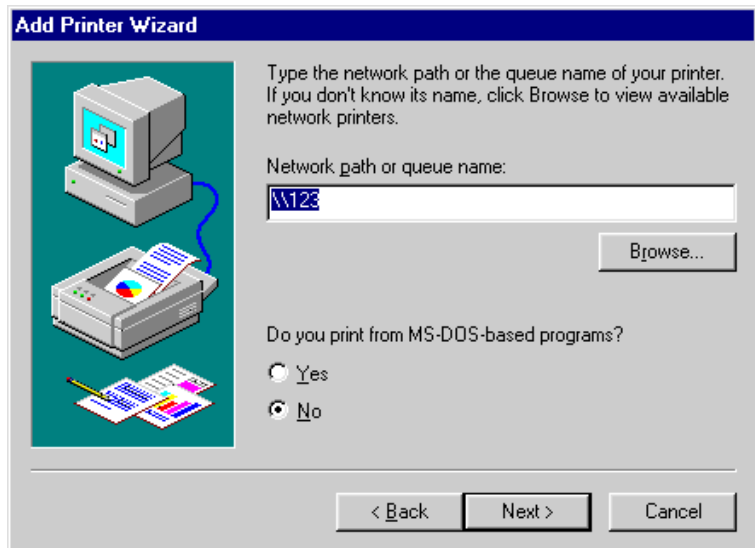
**To remove an existing printer port installation:**

1. Open Start - Settings - Control Panel - Add/Remove Programs
2. Look for an entry with a name like "Shared Port", "Shared Printer Port", "Print Server Driver" or "Print Server Port".
3. Select this item, click "Add/Remove", and confirm the deletion.

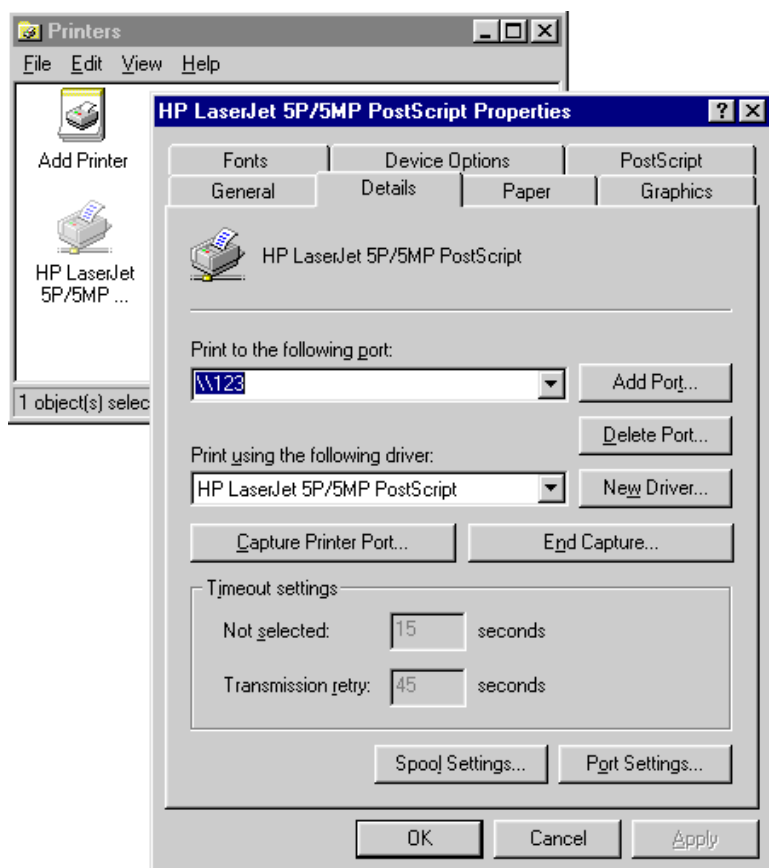
**Problem 2:** I am using Windows 95, and the Printing software installed and ran, but when I selected a port and clicked "Add"; the printer was not installed.

**Solution 2:** Try installing the printer using the standard Windows tools, as follows:

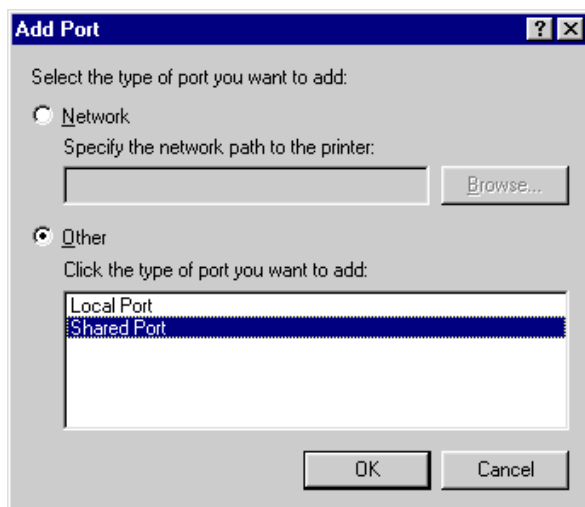
1. Start the *Add Printer Wizard*.
2. Select *Network Printer* when prompted "How is the printer attached to your Computer?", and click Next.
3. When prompted for the Network Path or Queue, enter a dummy value such as \\123, as shown below. (Do NOT select *Yes* for "Do you print from MS-DOS programs?")



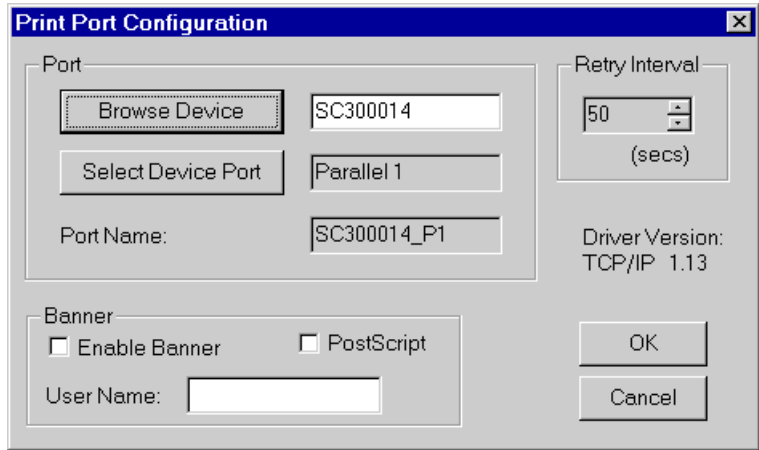
4. The printer wizard will display a message stating that "The Network Printer is off-line". This is OK. Continue the Add Printer Wizard until finished.
5. When finished, go to *Control Panel-Printers*. The printer icon will be grayed out indicating the printer is not ready.
6. Right-click the Printer, and select *Properties*. Then select the *Details* tab, as shown below.



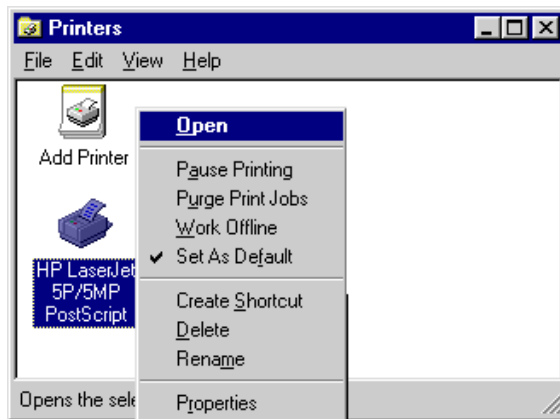
7. Click the *Add Port* button. On the resulting screen, select *Other*, then *Shared Port*, as the port to add, as shown below.



8. Click *OK* to see the *Print Port Configuration* screen, as shown below.



9. Click the *Browse Device* button, select the desired Wireless Gateway, and click OK.
10. Click OK to return to the Printers folders, and right-click on the Printer. Ensure that the *Work off-line* option is NOT checked.



The Printer should no longer be grayed out, and is ready for use.

**Problem 3:** On my Macintosh, the Wireless Gateway's printer is not listed.

**Solution 3**

Check the following:

- Ensure the network connection is working. If you can connect to the Wireless Gateway for configuration, then the connection is OK.
- Ensure the *Printer Object Type* on the Wireless Gateway's *Printer Port* screen is set correctly. If this is wrong, the printer will not be listed on the Macintosh. Check your printer manufacturer's documentation or Web site to determine the correct *Object Type* for your printer.



## Dial-in Access

**Problem 1:** Remote PC can't connect to the Wireless Gateway.

**Solution 1:** Check the settings on the Wireless Gateway

- Serial Port is Enabled.
- Dial-in is Enabled.
- User has been created, and has Dial-in permission.
- Call-back settings are correct for this user.
- Modem settings are correct.
- Both the Wireless Gateway and the remote PC are using the same settings for the login authentication (PAP, CHAP, MSCHAP).

### Check the Modem

- Modem is properly connected and powered on.
- The modem is working correctly, and the Remote user is dialing the correct telephone number for the modem.  
This can be checked by listening to the modem. You should hear the Wireless Gateway's modem answer the incoming call.
  - If the call is received but not answered, the modem's "Auto-answer" feature is turned OFF. To turn it on, add the appropriate AT command to the *Initial String* in the on the Wireless Gateway's *Modem Properties* screen. See Chapter 6 for details of the *Modem Properties* screen, and Appendix C for more information on AT commands.
  - If the call is answered, but no connection is established, then either the modems are unable to negotiate a connection, or the login to the Wireless Gateway has failed.  
This can be checked by examining the Log file for the Remote PC. See *Finding the current Initial String* in Appendix C for instructions on enabling and viewing the Log file.

### Check the Remote PC

- Ensure that both the Wireless Gateway and the remote PC are using the same settings for the login authentication (PAP, CHAP, MSCHAP).
- When prompted for "User Name" and "Password", the remote user must enter the correct *User Name* and *Password*, as configured on the Wireless Gateway's *User Details* screen.
- The modem Log file on the remote PC may provide useful information about the cause of the connection failure. See *Finding the current Initial String* in Appendix C for instructions on enabling and viewing the Log file.

**Problem 2:** Remote PC can connect using Dial-in, but can't access LAN resources.

**Answer 2:** Currently, Microsoft networking (using NetBIOS over TCP/IP) is not supported. Only standard TCP/IP connections can be made. So the Dial-in PC cannot use *Network Neighborhood*, or Windows File/Print sharing.

**Problem 3:**      **On the LAN, there is an IP Address conflict involving the Dial-in PC. How do I set the IP Address allocated to the Dial-in PC?**

**Answer 3:**      This problem can only occur if the Wireless Gateway's DHCP Server is Disabled.

In this situation, the DHCP Server must still allocate an IP Address to the Dial-in user. To set this IP Address:

1. Connect to the Wireless Gateway
2. On the *Quick Setup* screen, locate the DHCP Server section, and set both the *Start IP Address* and the *Finish IP Address* to the IP Address you wish to be assigned to the Dial-in user.
3. Save these settings.

## Appendix B



# About Wireless LANs

*This Appendix provides some background information about using Wireless LANs (WLANs).*

## Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

### Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

### Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.



**Note!**

**Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.**

## BSS/ESS

### BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

**Using the same SSID is essential.** Devices with different SSIDs are unable to communicate with each other.

### ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points **SHOULD** use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

## Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available.
- Client (PC) Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If your PC's wireless card does NOT automatically scan all wireless channels, then you must manually set it to the Channel used on the Access Point.

## WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

**If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:**

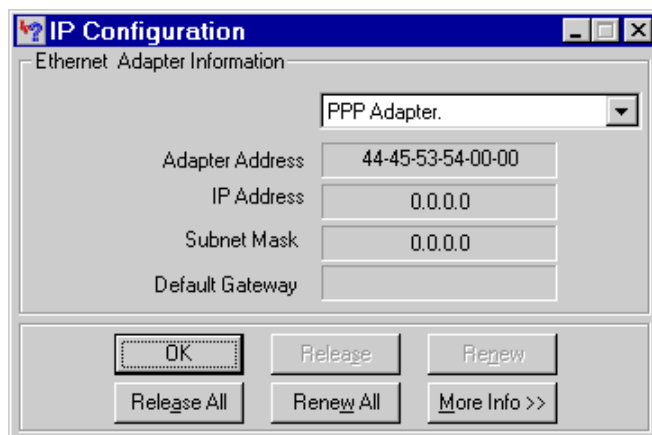
<b>WEP</b>	Off, 64 Bit, 128 Bit
<b>Key</b>	For 64 Bit encryption, the Key Table must match. For 128 Bit encryption, the Key value must match.
<b>WEP Authentication</b>	Open System or Shared Key.

## Access Control

The *Access Control* feature allows you to determine which Wireless Stations can use the Access Point. You need to identify each Wireless Station by its Hardware or physical Address.

On Windows, you can determine the Hardware (physical) Address using *WinIPCfg*, as follows:

1. Use *Start - Run* to open the "Run" dialog.
2. Type WINIPCFG and press Enter (or click OK).



**Figure 38: WinIpCfg**

3. WinIPCfg will then run, as shown above.
4. Select your Wireless adapter from the drop-down list, and check the *Adapter Address* field.

## Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

- Mode** On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
- SSID (ESSID)** Wireless Stations must use the same SSID (ESSID) as the Access Point they wish to connect to.
- WEP** The Wireless Stations and the Access Point must use the same settings for WEP (Off, 64 Bit, or 128 Bit).
- WEP Key:** If WEP is enabled, the Key Table (for 64 Bit encryption) or Key (for 128 Bit Encryption) must be the same on the Wireless Stations and the Access Point.
- WEP Authentication:** If WEP is enabled, all Wireless Stations must use the same setting as the Access Point (either "Open System" or "Shared Key").

# Appendix C

## AT Commands



### AT Commands

This Appendix details the "AT" commands used by modems and ISDN TAs. This information is provided to assist users who are using the Wireless Gateway's serial (RS232 port).

It is not relevant to Cable or DSL modems connected to the WAN (Ethernet) port.

### Required Settings

For the Wireless Gateway to use the Serial Port correctly, the modem or ISDN TA must be set as follows.

Setting	AT Command
Fixed baud rate setting	AT&B1
RTS/CTS flow control	AT&K3
DCD to track the presence of a carrier	AT&C1
DTR off to hang-up modem	AT&D2
DSR always on	AT&S0

If your Modem or ISDN TA uses the commands above, then the *Initial String* would be as follows:

```
AT&F&B1&K3&C1&D2&S0X4
```

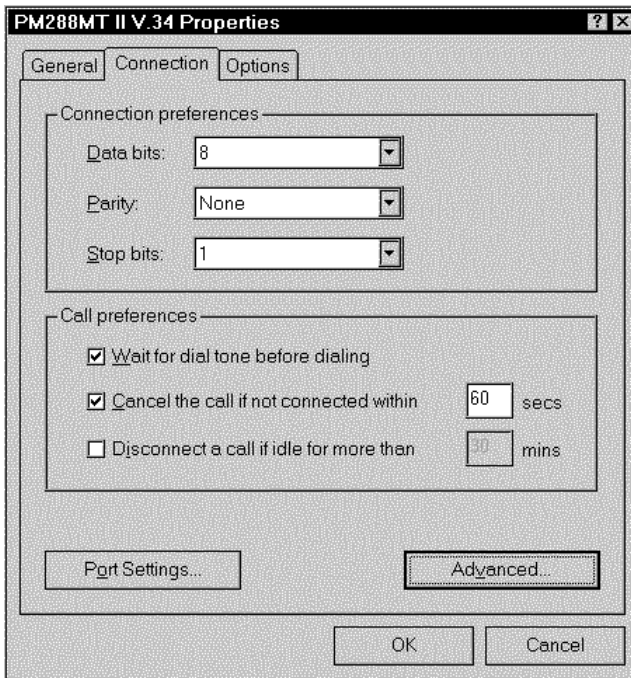
#### Notes:

- The command "AT&F" is used to set the modem to the factory default settings, to ensure a consistent starting point.
- For some Mircocom and other modems, the "ATX4" command is not sufficient - a "W2" command (no "AT") must be used as well.
- ISDN TAs may not use these commands; please check your user guide for your ISDN TA.

### Finding the current Initial String

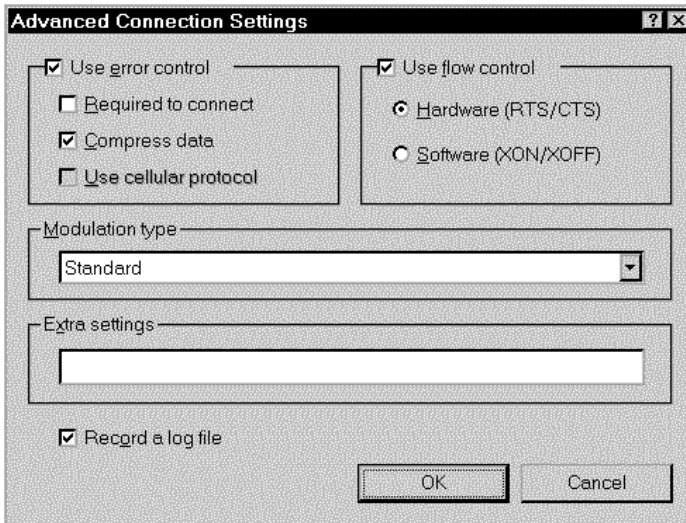
If your modem or ISDN TA is already working correctly using the PC's serial port, but you don't know what the initialization string is, you can use the following procedure to find out.

1. Select *My Computer*, then *Dial-Up Networking*.
2. Select the icon for your connection, then *Properties*.
3. Click the *Configure* button, then the *Connection* tab, as shown below.



**Figure 39: Connection Properties (W95/98)**

4. Select *Advanced* to see the screen below.



**Figure 40: Advanced Connection (W95/98)**

5. Check the option *Record a log file*. Then click *OK* and exit.
6. Use *Dial-up Networking* to make your on-line connection normally. A log file *MODEMLOG.TXT* will be created in your Windows directory.
7. Use Notepad or another editor to read and print the file *MODEMLOG.TXT*.
8. Examine the file to determine the *Initial String* value. It will be near the beginning of the file, and look something like the example shown previously.

## Standard AT Commands

Most modems use the standard AT commands, as shown in the following tables. Consult the manual for your modem to set what AT commands it supports.

Note that the trailing "n" in many commands indicates a number.

The allowable numbers, and their effect, are listed below the command.

Command	Description
<any key>	Terminate current connection attempt
+++	Escape sequence code, entered in data state, wait for modem to return to command state
ATA	Force answer mode on-line
ATBn	Handshake operation
B0	Select ITU-T V.22 for 1200 bps communication
B1	Select Bell 212A for 1200 bps communication
ATD	Dial number and options that follow
P	Pulse dial
T	Tone dial
,	Pause for a specified time
;	Return to command state after dialing
!	Hook flash, call transfer
W	Wait for second dial tone
@	Wait for 5-second silence before proceeding, otherwise return O ANSWER"
R	Reverse Dial (Originate a call in answer mode)
ATDL	Dial last number
ATDSn	Dial number stored in NVRAM at position <i>n</i> . ( <i>n</i> =0..9)
ATEn	Command mode local echo of keyboard commands
E0	Echo off
E1	Echo on
ATHn	On/Off hook control
H	Hang up modem
H0	Hang up (on hook), same as ATH
H1	Get off hook
ATIn	Display inquired information
I0	Display product code
I1	Display product information and ROM checksum
I2	Link status report



ATLn	Speaker volume control. n=0-7
ATMn	Speaker control
	M0 Speaker always off
	M1 Speaker on until carrier is detected
	M2 Speaker always on
	M3 Speaker on after last digit dialed, off at carrier detect
ATNn	Ring volume control, n=0 disables ring function. (n=0..7)
ATO	Return to on-line state
ATP	Pulse dial
ATQn	Result code displayed
	Q0 Modem returns result code
	Q1 Modem does not return result code
	Q2 Return result code but quiet in answer mode (will not show in AT&Vn)
ATS0=n	Number of rings required before modem answers. n=0 disables auto-answer.
ATSr.b=n	Set bit <i>b</i> of S-register <i>r</i> to <i>n</i> . (n=0 or 1)
ATSr.b?	Inquiry bit <i>b</i> of S-register <i>r</i>
ATSr=n	Set S-register <i>r</i> to value <i>n</i> , where <i>n</i> is a decimal number between 0-255
ATSr?	Display value stored in S-register <i>r</i>
ATT	Tone dial
ATVn	Verbal/Numeric result codes
	V0 Display result codes in numeric form
	V1 Display result codes in verbose form
ATXn	Result code options. (n=0..7)
ATZn	Reset the modem and set power-on profile. (n=0..4)
	Zn Reset modem and load user profile <i>n</i> (n=0..3)
	Z4 Reset modem and load factory settings
AT\$	Help, Basic command summary
AT&\$	Help, Extended AT& command summary
AT*\$	Help, Extended AT* command summary

## Extended "AT&" Commands

(Includes RTS/CTS Flow Control Commands)

Command	Description
&Bn	Data rate, terminal-to-modem
&B1	DTE/DCE rate fixed at DTE setting
&Cn	Carrier Detect operations
&C1	Carrier Detect tracks presence of carrier
&Dn	Data Terminal Ready (DTR) operations
&D2	DTR off causes modem to hang up
&F	Load the default factory settings,
&Kn	Data flow control, DTE/DCE, n=0,3,4
&K0	Flow control disabled
&K3	Hardware (RTS/CTS) flow control
&K4	Software (XON/XOFF) flow control
&Sn	Data Set Ready (DSR)
&S0	DSR overridden, DSR always on

# Appendix D

## Specifications



### Wireless Gateway

Models	MIL-W0311 & MIL-W1311
Dimensions	240mm(W) * 120mm(D) * 35mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	3 Ethernet: 2 * 10/100BaseT (RJ45) for LAN 1 * 10BaseT (RJ45) for WAN
PCMCIA Slot	1 Type II, 16bit bus
Wireless interface	Wireless Access Point via supplied PCMCIA card IEEE 802.11b compatible, WEP security support, roaming support
Printer Port	1 * parallel printer port
Serial Port	1 * RS232 9 pin male port
LEDs	9
Power Adapter	12 V DC External

#### FCC Statement:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

#### CE Marking Warning

This is a Class B product<sup>1</sup>. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

---

<sup>1</sup> Shielded (STP) network cable is required.

## PCMCIA Wireless Card (MIL-W1311 only)

Interface	PCMCIA 68pin, 16bit data
Standards	IEEE802.11b WLAN, PCMCIA 2.1, JEIDA 4.2
Frequency	2.4 to 2.4835GHz ( Industrial Scientific Medical Band )
Channels	Maximum 14 Channels, depending on regulatory authorities
Data Rate	11 / 5.5 / 2 / 1 Mbps
Coverage Area	Closed Space : 25m @11Mbps, 100m @5.5Mbps or lower
Power	DC +3.3V / 220mA
Output Power	13dBm (typical)
Receiver Sensitivity	-80dBm Min.
Operating Temperature	0° to 55°C
Storage Temperature	-25° to 70°C
Relative humidity	10% to 90%